高等学校计算机类国家级特色专业系列规划教材

信息安全管理与工程

王春东 主编
杨宏 莫秀良 岳丽 副主编

清华大学出版社

高等学校计算机类国家级特色专业系列规划教材

信息安全管理与工程

王春东　主编
杨　宏　莫秀良　岳　丽　副主编

清 华 大 学 出 版 社
北　京

内 容 简 介

本书以目前信息系统安全管理与工程存在的问题和发展要求为写作方向，以编者所在一线教师团队多年来相关教学以及研究工作为基础，系统阐述了信息安全管理与工程的体系结构、基本框架、法律规范等相关知识。全书共分为10章，各章内容既相互独立，又相互联系。第1章是信息安全管理体系；第2章详细介绍信息安全风险管理；第3章是基本信息安全管理；第4章是重要信息安全管理措施；第5章是信息安全管理华为典型实例；第6章是信息安全工程原理；第7章是信息安全工程实践；第8章是信息安全保障；第9章介绍信息安全标准；第10章详细阐述信息安全法律政策和道德规范。

本书可供信息安全、计算机科学与技术专业的本科学生，以及相关领域的研究人员、教师、研究生和工程技术人员参考。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目（CIP）数据

信息安全管理与工程/王春东主编. --北京：清华大学出版社，2016
高等学校计算机类国家级特色专业系列规划教材
ISBN 978-7-302-41636-4

Ⅰ. ①信…　Ⅱ. ①王…　Ⅲ. ①信息安全－安全管理－高等学校－教材　Ⅳ. ①TP309

中国版本图书馆CIP数据核字（2015）第228400号

责任编辑：汪汉友　赵晓宁
封面设计：傅瑞学
责任校对：李建庄
责任印制：刘海龙

出版发行：清华大学出版社
网　址：http://www.tup.com.cn，http://www.wqbook.com
地　址：北京清华大学学研大厦A座　**邮　编**：100084
社 总 机：010-62770175　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　销：全国新华书店
开　本：185mm×260mm　**印　张**：14.75　**字　数**：367千字
版　次：2016年6月第1版　**印　次**：2016年6月第1次印刷
印　数：1～2000
定　价：34.50元

产品编号：065799-01

前　言

随着信息化和网络化的发展，信息安全问题日益突出。“信息安全管理与工程”成为国内许多高校信息安全专业、计算机科学与技术专业的必备课程。目前国内关于信息安全管理及信息安全工程的书籍特别多，但这些书籍更多偏重于理论知识。本书理论联系实际，引用了业界典型信息安全管理案例，使内容更加充实。书中多处运用图形和表格来解释难懂的概念，图文并茂，易懂易学，非常适合不同水平的读者阅读。本书是作者及教学团队十余年来在信息安全管理与工程方面所做工作的总结。希望本书的出版，能为我国信息安全专业的发展、学科的建设和创新突破带来一些启迪和帮助。

由于作者水平有限，本书遗漏和不妥之处在所难免，恳请读者批评指正。

编　者

2016 年 4 月

目　　录

第 1 章　信息安全管理体系

导入语：本章系统地介绍了信息安全管理体系方面的内容，包括信息安全管理的基本概念和信息安全管理体系建设。信息安全管理的基本概念部分，介绍了信息安全管理的作用、风险管理的概念和作用、安全管理控制措施的概念和作用。信息安全管理体系建设部分，介绍了过程方法与 PDCA 循环，以及建立、运行、评审与改进 ISMS。

本章主要知识结构如图 1.1 所示。

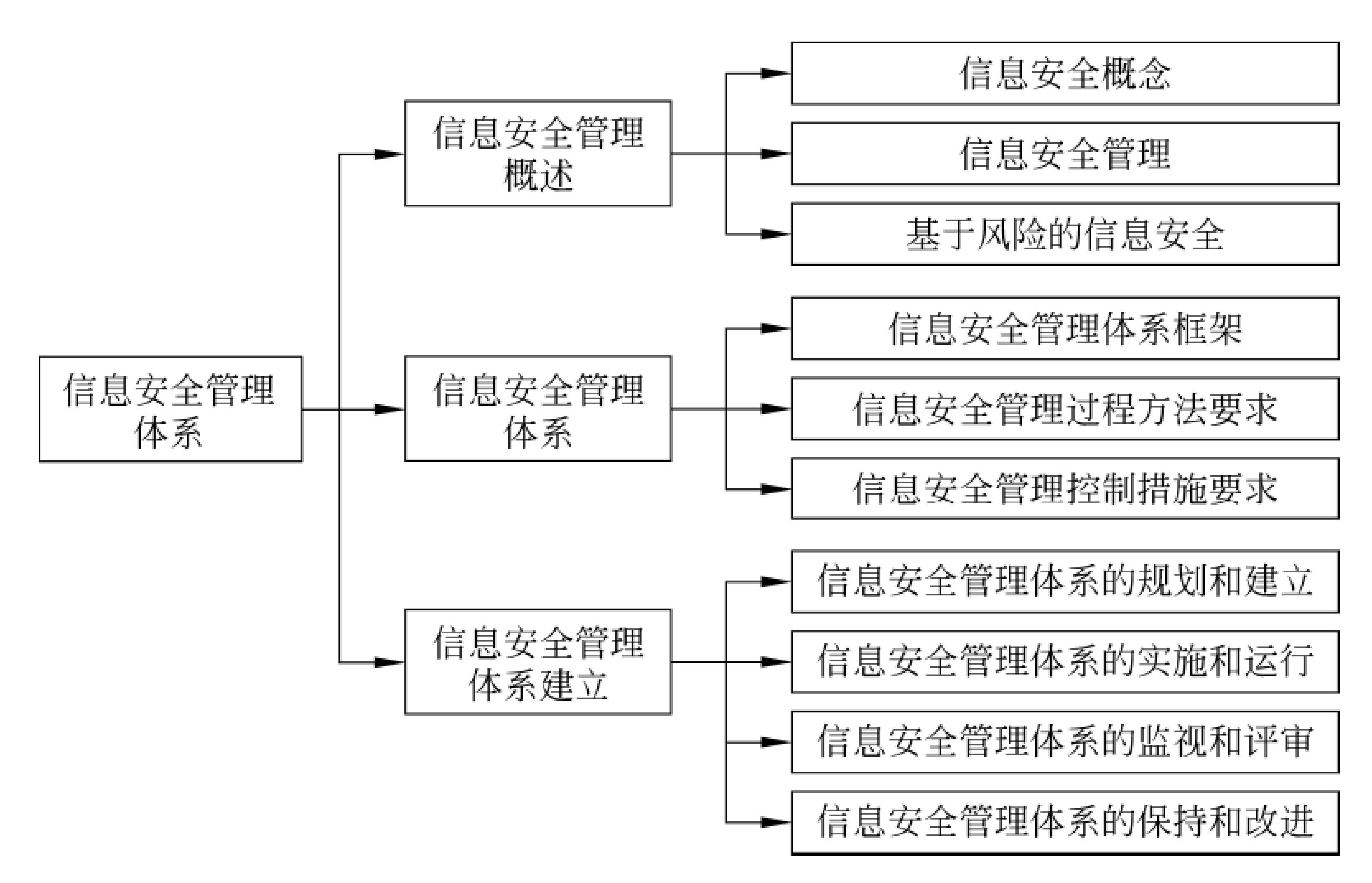


图 1.1　本章主要知识结构框图

考核目标：理解信息安全“技管并重”原则的意义与成功实施信息安全管理工作的关键因素。理解信息安全风险的概念，包括资产价值、威胁、脆弱性、防护措施、影响、可能性。理解风险评估是信息安全管理工作的基础。理解风险处置是信息安全管理工作的核心。理解安全管理控制措施是管理风险的具体手段。了解 11 个基本安全管理控制措施的基本内容。

1.1　信息安全管理概述

随着全球网络的持续发展，网际互联对于通信系统和计算系统的流畅运作变得愈发重要。然而，日益增多的病毒、蠕虫攻击事件以及黑客网络犯罪表明：当前的信息技术还存在诸多缺陷，因而有必要提高信息系统的安全。

信息安全管理是通过维护信息的保密性、完整性和可用性等来管理和保护信息资源的一项体制，是对信息安全保障进行指导、规范和管理的一系列活动和过程。

1.1.1　信息安全概念

客观世界是由物质、能量和信息三要素构成。现在人类社会进入了一个崭新的电子信

息化时代，信息安全变得越来越重要。

信息是一种资产，像其他重要的业务资产一样，它对组织具有价值，因此需要妥善保护。信息安全的含义是通过各种计算机、网络和密钥技术，保证在各种系统和网络中传输、交换和存储的信息的机密性、完整性和真实性。信息安全的结构层次分为物理安全、安全控制和安全服务。为了更好地理解信息安全管理，必须熟悉一个组织机构有价值的关键信息的特性。

（1）保密性。为了确保只有那些被授予特定权限的人才能够访问到信息，信息的保密性依据信息被允许访问对象的多少而不同。根据信息的重要程度和保密要求将信息分为不同密级，所有人员都可以访问的信息为公开信息，需要限制访问的信息为敏感信息或秘密信息。

（2）完整性。保证信息和处理方法的正确性和完整性。信息完整性一方面指在使用、传输、存储信息的过程中不发生篡改信息、丢失信息、错误信息等现象；另一方面指信息处理方法的正确性，执行不正当的操作，有可能造成重要文件的丢失，甚至整个系统的瘫痪。

（3）可用性。确保那些已被授权的用户在他们需要的时候，可以访问到所需信息，即信息及相关的信息资产在授权人需要的时候，可以立即获得。例如，通信线路中断故障、网络的拥堵等会造成信息在一段时间内不可用，影响正常的业务运营，这是信息可用性的破坏。提供信息的系统必须能适当地承受攻击并在被攻击后得到恢复。

1.1.2 信息安全管理

一个成功的信息安全项目，要将上述的各种概念结合起来，以减少信息资产的风险，必须通过细致的管理来实现。站在较高的层次上看信息和网络安全的全貌就会发现，安全问题实际上都是人的问题，单凭技术无法保证整个系统的安全。

信息安全管理的定义：组织中为了完成信息安全目标，针对信息系统，遵循安全策略，按照规定的程序，运用恰当的方法，而进行的规划、组织、指导、协调和控制等活动。

信息安全管理的目标如下：防止未授权存取；防止未被授权的人进入系统；用户意识、良好的口令管理、登录活动记录和报告、用户和网络活动的周期检查等都是防止未授权存取的关键；防止泄密，防止已授权和未授权的用户相互存取重要信息，这也是计算机安全的一个重要问题；防止用户拒绝系统的管理，这应由操作系统来完成，一个系统不应被一个有意试图使用过多资源的用户损害；防止丢失系统的完整性，这与系统管理员的实际工作和保持可靠的操作系统有关。

信息安全是一个多层面、多因素的过程。如果组织凭着一时的需要，想当然去制定一些控制措施和引入某些技术产品，都难免存在挂一漏万、顾此失彼的问题，使得信息安全这只“木桶”出现若干“短板”，从而无法提高信息安全水平。正确的做法是参考国内外相关信息安全标准与最佳实践过程，根据组织对信息安全的各个层面的实际需求，在风险分析的基础上引入恰当控制，建立合理安全管理体系，从而保证组织赖以生存的信息资产的保密性、完整性和可用性。

信息安全管理是通过维护信息的保密性、完整性和可用性，来管理和保护组织所有的信息资产的一项体制；是组织中用于指导和管理各种控制信息安全风险的一组相互协调的活动，有效的信息安全管理要尽量做到在有限的成本下，保证安全风险控制在可接受的范围。

1.1.3 基于风险的信息安全

安全管理是信息安全中非常重要的一环,要实现较完善的安全管理,必须分析、评估安全需求,建立满足需求的计划,实施这些计划,并进行日常维护和管理。由此可见,安全管理过程的第一步就是要建立一个全局安全目标,然后将其整合到机构的安全政策中去。实现这一要求的关键是对风险的评估,将风险减少到可以接受的水平。

1. 风险评估概述

识别了机构的威胁和漏洞后,就可以评估每个漏洞的相关风险了。这是通过风险评估过程来完成的。风险评估给每项信息资产分配一个风险等级或者分数。此数字可用于评估每项易受攻击的信息资产的相关风险,并在风险控制过程中促进比较等级的发展。

风险＝出现漏洞的可能性×信息资产的价值－当前控制减轻的风险概率
＋对漏洞了解的不确定性

其中,"出现漏洞的可能性"是指成功攻击机构内某个漏洞的概率。在风险评估中,要给成功攻击漏洞的可能性指定一个数值。国家标准与技术协会在 Special Publication 800-30 中推荐,这个可能性应指定为 0.1～1.0 之间的一个值。比如,在室内被陨石击中的可能性是 0.1。明年收到至少一封带病毒或蠕虫的电子邮件的可能性是 1.0。还可以选择使用 1～100 中的数字,但不能使用 0,因为可能性为 0 的漏洞已从资产/漏洞列表中删除。

2. 信息安全风险评估原则

1)自主

自主指组织机构内部的人员管理和指导组织机构的信息安全风险评估。这些人负责指导风险管理活动,并对组织机构的安全工作做出决策。这种方法使评估能够考虑组织机构的与众不同的情形和环境。自主要求:通过领导信息安全风险评估并对评估过程进行管理,负责信息的安全。最终对组织机构的安全工作做出决策,包括实现哪些改进和采取哪些行动。

2)适应度量

一个灵活的评估过程可以适应不断变化的技术和进展,既不会受限于当前威胁源的严格模型,也不会受限于当前公认的"最佳"实践。因为信息安全和信息技术领域变革非常迅速,所以需要一个适应性强的度量集,组织机构及其独特的环境可以据此进行评估。适应度量要求:定义公认的安全实践、已知的威胁源和技术缺陷目录;能适应信息目录变化的评估过程。

3)已定义过程

已定义的过程描述了信息安全评估程序依赖于已定义的标准化评估规程的需要。使用一个已定义的评估过程有助于过程的制度化,保证评估的应用能达到一定程度的一致性。一个已定义的过程要求:为执行评估分配责任;定义所有的评估活动;规定评估过程所需的所有工具、工作表和信息目录;为记录评估结果创建通用的格式。

4)连续过程的基础

组织机构必须实施基于实践的安全策略和计划,以便逐渐改进自身的安全状态。通过实施这些基于实践的解决方案,组织机构就能够开始将最佳的安全实践制度化,使其成为组织机构日常开展业务方法的一部分。安全改进是一个连续的过程,信息安全风险评估的结

果为连续的改进奠定了基础。它需要：使用已定义的评估过程标识出信息安全风险；实施信息安全风险评估的结果；逐步培养管理信息安全风险的能力；实施安全策略和计划，使安全改进结合基于实践的方法。

3. 信息安全风险评估的目标

(1) 了解信息系统的体系结构和管理水平，以及可能存在的安全隐患。

(2) 了解信息系统所提供的服务及可能存在的安全问题。

(3) 了解其他应用系统与此信息系统的接口及相应的安全问题。

(4) 网络攻击和电子欺骗的模拟检测和预防。

(5) 找出目前的安全控制措施与安全需求的差距，并为其改进提供参考。

4. 风险评估的过程

(1) 信息资产评估。使用信息资产的识别过程中得到的信息，就可以为机构中每项信息资产的价值指定权重分数。根据机构的需要，使用的数字可以不同。一些团体使用1～100的权重分数，其中100代表在几分钟内就会使公司停止运转的信息资产。还有的团体使用1～10的权重分数，或者用1、3和5代表低、中和高价值的资产。也可以根据自己的需要建立权重值。

(2) 风险的确定。信息资产风险的计算公式如下：

风险＝信息资产的价值(或影响)×出现漏洞的可能性－已控制风险的比例＋不确定因素

例如，信息资产 A 的价值是50，有1个漏洞，漏洞1出现的可能性是1.0，当前没有控制风险，估计该假设和数据的准确率为90%。信息资产 B 的价值是100，有2个漏洞，漏洞2出现的可能性是0.5，当前已控制的风险比例是50%；漏洞3出现的可能是0.1，当前没有控制风险，估计该假设和数据的准确率为80%。这3个漏洞的风险等级分别如下：

资产 A：漏洞1的风险等级 $= (50 \times 1.0)(1 - 0\% + 10\%)$
$= (50 \times 1.0) \times 1 - (50 \times 1.0) \times 0\% + (50 \times 1.0) \times 10\%$
$= 50 + 0 + 5 = 55$

资产 B：漏洞2的风险等级 $= (100 \times 0.5)(1 - 50\% + 20\%)$
$= (100 \times 0.5) \times 1 - (100 \times 0.5) \times 50\%$
$+ (100 \times 0.5) \times 20\%$
$= 50 - 25 + 10 = 35$

资产 B：漏洞3的风险等级 $= (100 \times 0.1)(1 - 0\% + 20\%)$
$= (100 \times 0.1) - (100 \times 0.1) \times 0\% + (100 \times 0.1) \times 20\%$
$= 10 - 0 + 2 = 12$

(3) 识别可能的控制。对于每一个威胁及其残留风险的相关漏洞而言，应该建立一份控制计划的初步列表。残留风险是指使用了现有的控制方法后信息资产残留的风险。控制的一种特殊应用是访问控制，它主要控制用户进入机构信息区域。这些区域包括信息系统、物理限制区域，如机房、甚至整个机构。访问控制通常由政策、计划和技术组成。访问控制有许多方法，访问控制可以是强制的、非任意的和任意的。每种方法都针对一组控制，以便管理对某类信息或信息集合的访问。

(4) 记录风险评估的结果。在风险评估过程结束时，将得到一份很长的信息资产列表，其中包含这些信息资产的各种数据。到目前为止，这个过程的目标是识别机构中有某些漏

洞的信息资产，并将它们列出来，依照最需要保护的顺序划出等级。在准备这个列表时，需要收集和存储资产、资产面临的威胁和包含的漏洞等许多信息，还应收集已有控制的一些信息。漏洞风险等级表如表1.1所示。表中列出了每项易受攻击的资产，显示了权重因子分析表中此项资产的价值。在这个例子中，数字从1～100，并列出了每个不可控的漏洞及其出现的可能性，并计算出风险等级因子。从表中可以看出，最大的风险来自易受攻击的邮件服务器。尽管由客户服务电子邮件所代表的信息资产的影响等级仅为55，但是硬件相对较高的故障率使它成为最紧迫的问题。

表1.1　漏洞风险等级表

资　产	资产影响或相关价值	漏　洞	漏洞出现的可能性	风险等级因子
通过电子的客户服务请求(输入)	55	由于硬件故障而导致电子邮件中断	0.2	11
通过SSL客户订单(输入)	100	由于Web服务器硬件故障而导致订单丢失	0.1	10
通过SSL的客户订单(输入)	100	由于Web服务器或ISP服务故障而导致订单丢失	0.1	10
通过电子的客户服务请求(输入)	55	由于SMTP邮件转发攻击而导致电子邮件中断	0.1	5.5
通过电子的客户服务请求(输入)	55	由于ISP服务失败而导致电子邮件中断	0.1	5.5
通过SSL的客户订单(输入)	100	由于Web服务器拒绝服务攻击而导致订单丢失	0.025	4.5
通过SSL的客户订单(输入)	100	由于Web服务器软件故障而导致订单丢失	0.01	1

既然完成了风险识别过程，那么此过程的文件包含的内容应该是什么呢？为风险识别规划的过程应该指明此报告的作用、负责准备报告的人员以及检查这些报告的人员。漏洞风险等级表是风险管理过程下一阶段(评估并控制风险)的初始工作文件。表1.2显示了信息安全项目准备的标本表。

表1.2　风险识别及评估成果

成　果	用　途
信息资产分类表	集合信息资产以及它们对机构的影响或价值
权重标准分析表	为每项信息资产分配等级值或影响权重
漏洞风险等级表	为每对无法控制的资产漏洞分配风险等级

5. 风险控制策略

当机构管理人员发现信息安全威胁的风险产生了竞争劣势时，就通过信息技术和信息安全利益团体来控制风险，一旦该团体建立了漏洞等级表，就可以选择4项基本策略中的一项来控制这些漏洞产生的风险。这4个策略如下：

(1) 采取安全措施，消除或者减少漏洞的不可控制的残留风险(避免)。

(2) 将风险转移到其他区域，或者转移到外部(转移)。

(3) 减少漏洞产生的影响(缓解)。

(4) 了解产生的后果,并接受没有控制或者缓解的风险(接受)。

避免是试图防止漏洞被利用的风险控制策略。这是一种首选的方法,通过对抗威胁、排除资产中的漏洞、限制对资产的访问和加强安全保护措施来实现。

转移是将风险转移到其他资产、其他过程或其他机构的控制方法。它可以通过重新考虑如何提供服务、修改部署模式、外包给其他机构、购买保险或与提供商签署服务合同来实现。这样,机构就可以将管理复杂系统的风险转嫁给对处理这些风险有经验的另一个机构。使用专业合同的一个好处是提供商对灾难恢复负责,并通过服务级别协定来保证服务器和网站的可用性,但是外包并非不存在风险。信息资产的所有者、IT 管理人员和信息安全组要保证外包合同中的灾难恢复要求足够多,并在进行恢复工作前得到满足。如果外包商没有履行合同条款,结果就可能比预计的要糟糕得多。

缓解是一种控制方法,它试图通过规划和预先的准备工作,来减少漏洞造成的影响。这种方法包括 3 类计划,即事件响应计划(IRP)、灾难恢复计划(DRP)和业务持续性计划(BCP)。每种计划都取决于尽快检测和响应攻击的能力,依赖于其他计划的建立和质量。缓解起源于早期发现的攻击和机构快速、高效的响应能力缓解策略如表 1.3 所示。

表 1.3 缓解策略

计 划	描 述	实 例	何时使用	时间范围
事件响应计划(IRP)	在事件(攻击)进行过程中机构采取的行动	• 灾难发生期间采取的措施 • 情报收集 • 信息分析	当事件或者灾难发生时	立即并实时做出响应
灾难恢复计划(DRP)	发生灾难时的恢复准备工作;灾难发生之前及过程中减少损失的策略;逐步恢复常态的具体指导	• 丢失数据的恢复过程 • 丢失服务的重建过程 • 结束过程来保护系统和数据	在事件刚刚被确定为灾难后	短期恢复
业务持续性计划(BCP)	当灾难的等级超出 DRP 的恢复能力时,确保全部业务继续动作的步骤	• 启动下级数据中心的准备步骤 • 在远程服务位置建立热站点	在确定灾难影响了机构的持续运转之后	长期恢复

与缓解不同,接受风险是选择对漏洞不采取任何保护措施,接受漏洞带来的结果。这可能是一个明智的业务决策,也可能不是。这种策略的有效使用只有在机构进行以下工作之后:

(1) 确定了风险等级。

(2) 评估了攻击的可能性。

(3) 估计了攻击带来的潜在破坏。

(4) 进行了全面的成本效益分析。

(5) 评估了使用每种控制的可行性。

(6) 认定了某些功能、服务、信息或者资产不值得保护。

这种控制,或者说不进行控制,是基于这样一种结论:保护资产的成本抵不上安全措施的开销。

如果机构中每个已识别的漏洞都通过接受策略来处理,就说明该机构没有能力采取安

全措施，总体上对安全是漠不关心的。机构不能将无知当作一种理由，以不知道有责任保护员工客户的信息为借口，来避免被起诉。管理人员不能认为，如果他们不保护信息，攻击者就会觉得通过攻击不会获得有价值的信息。

理解了用于控制风险的策略，下面需要选择正确的策略，防范特定信息资产中的特定漏洞。

6. 选择风险控制策略

风险控制要为每个漏洞选择 4 个风险控制策略中的一个。在信息系统设计好后，就可弄清这个受保护的系统是否存在漏洞，是否可以利用。如果答案是肯定的，并且存在威胁，就要检查攻击者可以从成功的攻击中获得什么。要确定这个风险是否能接受，应估算该风险会对机构造成多大的损失。

下面介绍选择策略的一些规则作为进一步的指导。在计算不同策略的益处时，要注意威胁的等级和资产的价值在策略选择中有着非常重要的作用。

存在漏洞（缺陷或者缺点）：实现安全控制，来减少漏洞被利用的可能性。

（1）漏洞可以利用。应用分层保护、结构设计和管理控制，使风险降至最小或者防止风险发生。

（2）攻击者的开销少于收益。通过保护来增加攻击者的成本（如使用系统控制限制系统用户能够访问的资源，从而明显减少攻击者的收益）。

（3）可能的损失非常大。应用设计原理建筑设计、技术和非技术保护手段，来限制攻击的范围，从而减少可能的损失。

一旦实现了控制策略，就应对控制效果进行监控和衡量，来确定安全控制的有效性，估计残留风险的准确性。注意这个循环不会终止，只要机构继续运转，这个过程就会继续。并不是每个机构都有共同的意向和预算，通过应用控制对每个漏洞进行管理。所以，每个机构必须定义其可能碰到风险的等级。

风险可接受程度的定义如下：当机构评估绝对安全与无限制访问之间达到平衡时愿意接受的风险的级别和种类。例如，一家金融服务公司由政府管理，比较保守，希望应用各种合理的控制，甚至一些带有攻击性的控制来保护它的信息资产。另一个不由政府管理的公司也比较保守，希望避免在漏洞对完整性的损害方面进行负面报道。因此防火墙经销商可能制定比正常情况严厉得多的一组防火墙规则，因为在客户看来，被攻击后的消极结果是灾难性的。其他机构可能因为无知而带来非常危险的风险。针对风险，一个合理的方案是平衡暴露漏洞可能造成的损失和控制这些漏洞的开销。

即使机构尽可能地控制各种漏洞，仍然存在一些风险未能够完全排除、缓解或规划，这称为残留风险。换言之，残留风险是：

（1）降低了通过安全措施减小威胁效果的一种威胁。

（2）降低了通过安全措施减少漏洞效果的一种漏洞。

（3）降低了通过安全措施保护资产价值的效果的一种资产。

必须在机构内部判定残留风险的重要性，尽管这是违反直觉的，信息安全的目标并不是将残留风险降低为 0，而是将残留风险保护在机构可以控制的范围内。如果决定者发现有未受控制的风险，而各利益团体内部的权威机构决定不再理睬残留风险，这个信息安全计划就达到了它的主要目的。

系统报告的另一个方法是，在行动计划中证明每对信息资产/威胁的控制策略达到了预期的结果。这个行动计划包括具体的任务，每项任务分配给一个机构单位或者个人。它可能包括硬件和软件需求、预算估计以及具体要求的时间表，来启动时间控制所需的项目管理工作。

某些情况下，要为特定的 IT 项目进行风险评估。有时这是在 IT 项目经理的要求下完成的，因为机构政策要求这么做，或者因为这是很好的项目管理实验。有时，如果审计员或高级管理人员认为，IT 项目偏离了机构的信息安全目标，就可能要求进行项目的风险评估。项目的风险评估应在完成的 IT 系统中找出风险的来源，并为控制风险提出建议，因为这些风险可能会阻止项目的完成。例如，新应用程序常常需要在系统设计阶段进行项目风险评估，在完成项目的过程中，也要定期进行项目的风险评估。

最后，当管理人员需要某个信息系统主题的详细信息和机构面临的风险信息时，就可以在特定主题报告中进行风险评估。这些通常是向高级管理人员汇报时必须准备的报告，主要探讨信息系统操作风险的狭窄领域。例如，给管理人员报告新产生的漏洞，然后进行特定的风险评估。

7. 风险评估的相关要素

风险评估的相关要素为资产、威胁、脆弱性、安全风险、影响、安全控制措施以及安全需求。

（1）资产是指对组织具有价值的信息或资源，是安全策略保护的对象。资产能够以多种形式存在，包括有形的或无形的、硬件或软件、文档或代码以及服务或形象等诸多表现形式。在信息安全体系范围内为资产编制清单是一项重要的工作，每项资产都应该清晰地定义、合理地估价，并明确资产所有权关系，进行安全分类，记录在案。根据资产的表现形式，可将资产分为软件、硬件、服务、流程、数据、文档、人员等。

（2）威胁是指可能对组织或资产导致损害的潜在原因。威胁主要来源于环境因素和人为因素，其中人为因素包括恶意的和非恶意人员。

（3）脆弱性是指可能被威胁所利用的资产或若干资产的薄弱环节，如操作系统存在漏洞、数据库的访问没有访问控制机制、系统机房没有门禁系统等。脆弱性本身并不对资产构成危害，但是在一定条件得到满足时，脆弱性会被威胁加以利用来对信息资产造成危害。

（4）资产、威胁和脆弱性是信息安全风险的基本要素，是信息安全风险存在的基本条件，缺一不可。

（5）影响主要是指安全风险对业务的影响，即威胁利用资产的脆弱性导致资产价值损失等不期望发生事件的后果。

（6）安全控制措施是指为保护组织资产、防止威胁、减少脆弱性、限制安全事件的影响、加速安全事件的检测及响应而采取的各种实践、过程和机制。安全控制措施的实施领域包括组织政策与资产管理、物理环境、技术控制和人员管理等方面。

（7）安全需求是指为保证组织业务战略的正常运作而在安全控制措施方面提出的要求，风险评估是信息安全管理的基础，没有风险评估，信息安全管理体系的建立就没有依据。

1.2 信息安全管理体系

为了系统、全面、高效地解决网络与信息安全问题，英国标准协会（BSI）于1995年制订了《信息安全管理体系标准》，并于1999年进行了修订改版，2000年12月，经包括中国在内的国际标准组织成员国投票表决，目前该标准的第一部分已正式转化成国际标准。

具体说来，该标准内容包括信息安全政策、信息安全组织、信息资产分类与管理、个人信息安全、物理和环境安全、通信和操作安全管理、存取控制、信息系统的开发和维护、持续运营管理等。

信息安全管理体系（ISMS）是一个系统化、程序化和文件化的管理体系，属于风险管理的范畴，体系的建立基于系统、全面、科学的安全风险评估。ISMS体现预防控制为主的思想，强调遵守国家有关信息安全的法律法规及其他合同方要求，强调全过程和动态控制，本着控制费用与风险平衡的原则，合理选择安全控制方式保护组织所拥有的关键信息资产、确保信息的保密性、完整性和可用性，保持组织的竞争优势和商务运作的持续性。信息安全管理体系的过程如图1.2所示。

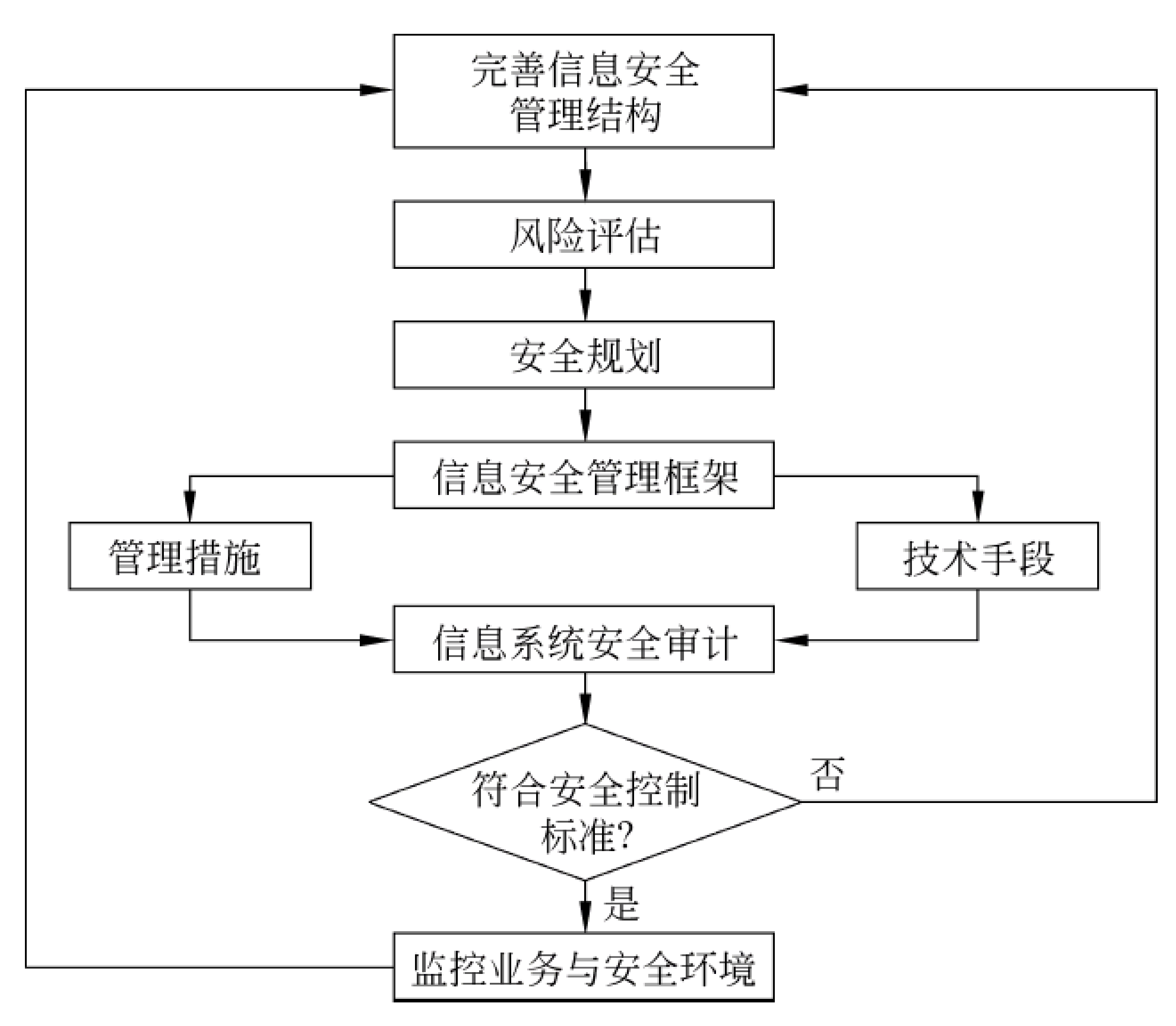


图1.2 信息安全管理体系的过程框图

1.2.1 信息安全管理体系概述

信息安全管理体系（Information Security Management System，ISMS）是组织在整体或特定范围内建立的信息安全方针和目标，以及完成这些目标所用的方法和体系。它是直接管理活动的结果，表示为方针、原则、目标、方法、计划、活动、程序、过程和资源的集合。

1. 信息安全管理体系的特点

（1）信息安全管理体系要求组织通过确定信息安全管理体系范围，制定信息安全方针，明确管理职责，以风险评估为基础选择控制目标和措施等一系列活动来建立信息安全管理体系。

（2）体系的建立基于系统、全面、科学的安全风险评估，体现以预防控制为主的思想，强调遵守国家有关信息安全的法律、法规及其他合同方面的要求。

（3）强调全过程和动态控制，本着控制费用与风险平衡的原则合理选择安全控制方式；强调保护组织所拥有的关键性信息资产，而不是全部信息资产，确保信息的保密性、完整性和可用性，保持组织的竞争优势和业务的持续性。

2. 信息安全管理体系的作用

（1）对组织的关键信息资产进行全面、系统的保护，维持竞争优势。

（2）在信息系统受到侵袭时，确保业务持续开展并将损失降到最低程度。

（3）促使管理层贯彻信息安全管理体系，强化员工的信息安全意识，规范组织信息安全行为。

（4）使组织的生意伙伴和客户对组织充满信心。

（5）组织可以按照安全管理，达到动态的、系统的、全员参与、制度化的、以预防为主的信息安全管理方式，用最低的成本，达到可接受的信息安全水平，从根本上保证业务的持续性。

1.2.2　信息安全管理体系的框架

信息安全管理体系是 PDCA 动态持续改进的一个循环体。PDCA 循环又名戴明环，是美国质量管理专家休哈特博士首先提出的，由戴明采纳、宣传，获得普及，它是全面质量管理所应遵循的科学程序。全面质量管理活动的全部过程，就是质量计划的制订和组织实现的过程，这个过程就是按照 PDCA 循环，不停顿地运转的。

ISMS 的 PDCA 具有以下内容：

（1）规划（Plan），即建立 ISMS。建立与管理风险和改进信息安全有关的 ISMS 方针、目标、过程和规程，以提供与组织总方针和总目标相一致的结果。

（2）实施（Do），即实施和运行 ISMS。实施与运行 ISMS 方针、控制措施、过程和规程。

（3）检查（Check），即监视和评审 ISMS。对照 ISMS 方针、目标和实践经验，评估并在适当时测量过程的执行情况，并将结果报告管理者以供评审。

（4）处置（Act），即保持和改进 ISMS。基于 ISMS 内部审核和管理评审的结果或其他相关信息，采取纠正措施以持续改进 ISMS。

ISMS 的 PDCA 具有以下特点：

（1）按顺序进行，它靠组织的力量来推动，像车轮一样向前进，周而复始，不断循环。

（2）组织中的每个部分，甚至个人，均可以 PDCA 循环，大环套小环，一层一层地解决问题。

（3）每通过一次 PDCA 循环，都要进行总结，提出新目标，再进行第二次 PDCA 循环。

1.2.3　信息安全管理过程方法要求

过程方法要求（Methodological Requirements）：为组织根据业务风险建立、实施、运行、监视、评审、保持和改进文件化的信息安全管理体系规定了要求，如图 1.3 所示。

按照 PDCA 循环理念运行的信息安全管理体系是从过程上严格保证了信息安全管理体系的有效性，在过程上的这些要求是不可或缺的，也就是说不是可选的，是必须执行的。

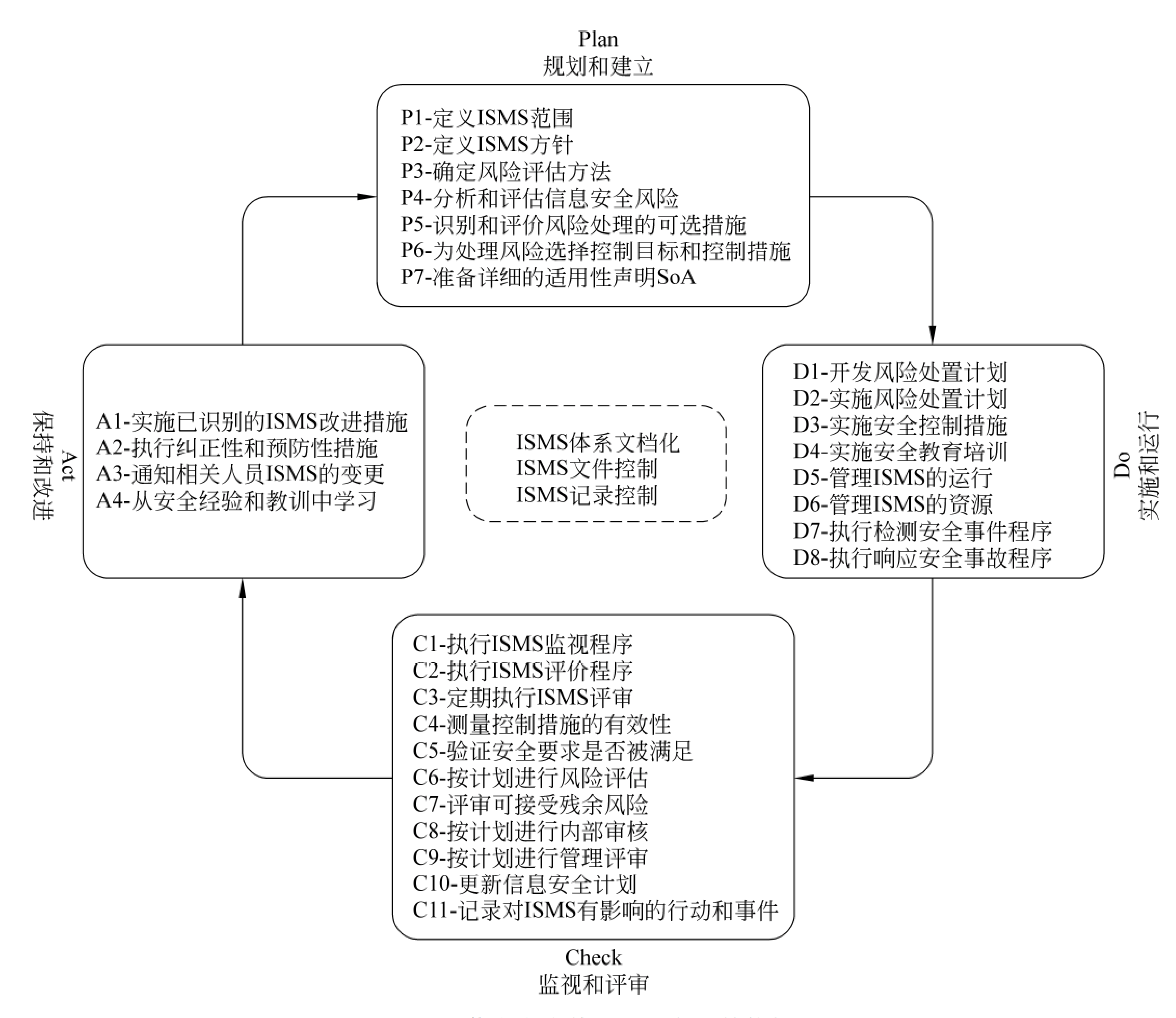


图 1.3　信息安全管理过程方法结构框图

1.2.4　信息安全管理控制措施要求

信息安全控制措施是组织为解决某方面信息安全问题的目的、范围、流程和步骤的集合，可以理解为信息安全策略，如防病毒策略、防火墙策略、访问控制策略等。

安全控制要求为组织选择满足自身信息安全环境要求的控制措施提供了一个最佳实践集。组织应根据法律法规的约束、自身的业务和风险特征选择适用的控制措施。当然组织也可以根据自身的特定要求对安全控制措施进行补充。

对控制目标与控制措施的选择应当由安全需求来驱动，选择过程应该是基于最好的满足安全需求，同时要考虑风险平衡与成本效益的原则，并且要考虑信息安全的动态系统工程过程，对所选择的控制目标和控制措施要及时加以校验和调整，以适应不断变化的情况，使信息资产得到有效的、经济的、合理的保护。

1.3　信息安全管理体系建立

1.3.1　信息安全管理体系的规划和建立

信息安全管理框架的建立应依照相应的程序进行。各组织机构所搭建的信息安全管理框架应根据自身状况，适应自身业务发展和信息安全的需求，并在正常的业务开展过程中具体实施所构架的 ISMS。与此同时，还应建立起各种与信息安全管理框架相一致的相关文档、文件，并进行严格管理，准确地记录在具体实施 ISMS 的过程中所出现的各种信息安全事件和安全状况，并建立严格的回馈流程和制度。具体的建立流程如图 1.4 所示。

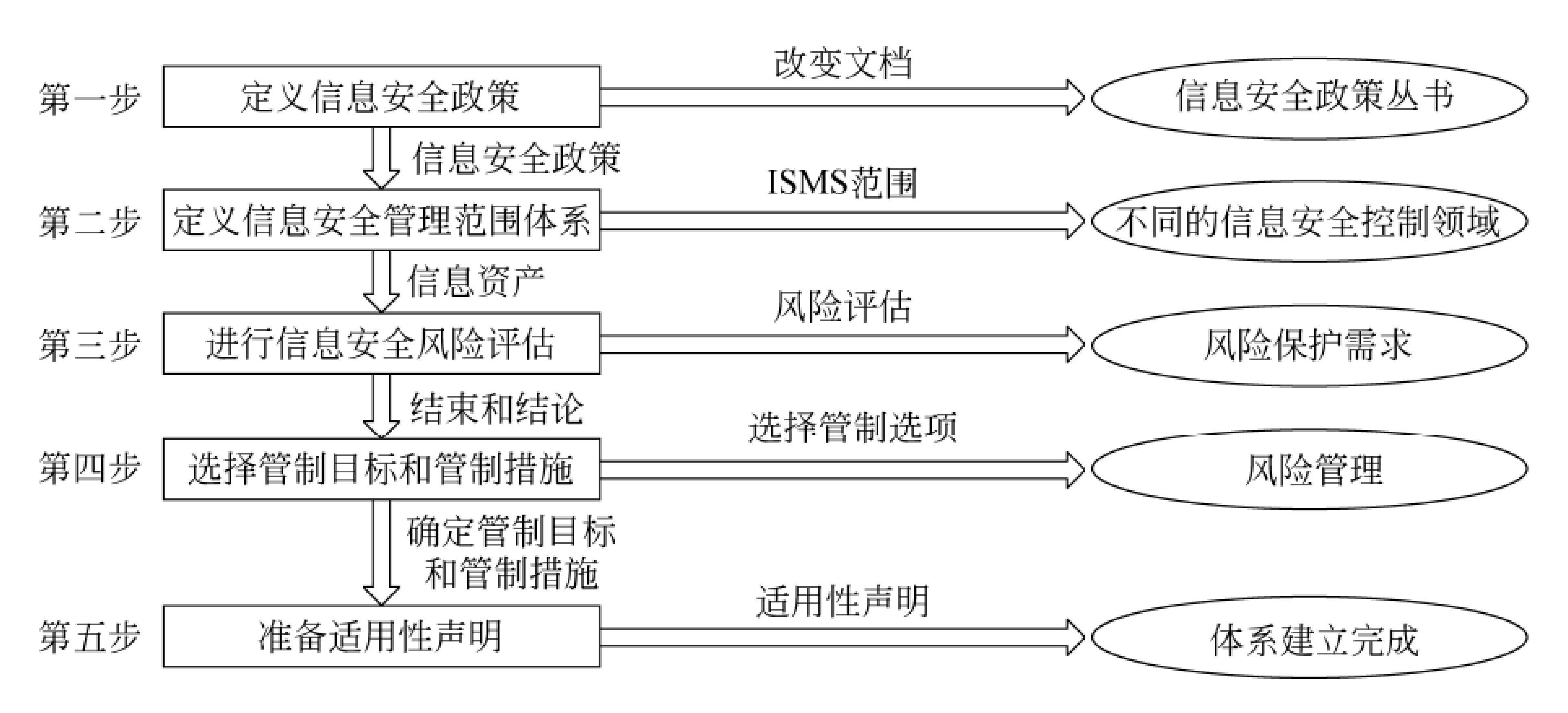


图 1.4　建立信息安全管理体系的流程

1. 定义信息安全政策

对于一个规模较小的组织机构，可以只制定一个信息安全政策，其应对组织机构内所有部门、员工适用；在规模相对较大的组织机构中，有时需要分别制定不同的信息安全政策，以适应组织机构内各个部门的实际情况。如果组织机构是一个集团公司，就需要制定一个信息安全政策丛书，分别适用于不同的子公司或各分支机构。但是，无论何种情况，信息安全政策都应避免将组织机构内所有层面的安全方针全部合并在一个政策中，同时要做到简洁明了、通俗易懂并直指主题。

2. 定义 ISMS 的范围

定义 ISMS 的范围，就是在组织机构内选定构架 ISMS 的范围。定义 ISMS 范围时，需要考虑的最重要因素是一个单位现有的组织结构，组织机构可能会根据自己的实际情况，只把 ISMS 构架在相关的部门或领域中，所以，在信息安全范围定义阶段，应将组织机构划分成不同的信息安全控制领域，从而便于组织机构对有不同需求的领域进行适当的信息安全管理。

在定义 ISMS 范围时，为了使 ISMS 定义得更加完整，应重点考虑组织机构以下的实际情况：

（1）组织机构现有部门。组织机构内现有部门和人员均应根据组织机构的信息安全政策和方针，担负起各自的信息安全职责。

（2）处所。具有多处所业务的组织机构单位，应该考虑不同业务处所对信息安全的不

同需求及其所面临的各种不同的信息安全威胁。

(3) 资产状况。在不同地点从事商务活动时,应把在不同地点涉及的信息资产纳入到ISMS管理范围内。

(4) 所采用的技术。使用不同计算机技术和通信技术,将会对信息安全范围的划分产生很大的影响。

3. 进行信息安全风险评估

信息安全风险评估的复杂程度取决于受保护的资产对安全的敏感程度和所面临风险的复杂程度,所采用的评估措施应与组织机构对信息资产风险的保护需求相一致。具体有以下3种风险评估方法可供选择。

1) 基本风险评估

只参照标准所提到的风险项对组织机构的资产进行风险评估的方法。此标准列出了一些常见的信息资产所面对的风险和管制要点,这些要点对一些中小企业(如业务性质相对简单,对信息、信息处理和计算机网络的依赖性不强或者不从事外向型经营的企业)的风险评估已经足够,但对不同组织机构来讲,基本的风险评估就可能会出现一些问题。一方面,如果该组织机构的安全级别设置太高,选择一些风险的管制措施将花费较大代价,而且可能使日常操作受到一定的限制;但如果级别设置太低,对一些风险的管制力又可能不足。另外,可能会给与信息安全管理有关的调整带来困难。因为在更新或调整信息安全管理系统时,可能难以评估旧的管制措施是否仍然符合现行的安全需求。

2) 详细风险评估

该方法首先对组织机构的信息资产进行详细的分类并赋值,然后根据不同的信息资产所面临的不同风险,详细划分对这些资产所造成的威胁等级和相关的脆弱性等级,并利用这些信息来评估系统存在的风险,从而对下一步管制措施的选择起到指导作用。一个组织机构对安全风险研究得越精确,安全需求也越清晰。与基本风险评估相比,详细风险评估将花费更多的时间和精力,有时还需要特定的专业技术知识以及外部组织机构的协助才能获得评估结果。

3) 基本风险评估和详细风险评估相结合

首先,根据基本的风险评估方法,确定信息安全管理系统范围内的潜在的高风险或对组织机构商业运作起关键作用的资产。在此基础上,信息安全管理系统范围内的资产分为两类:一类是仅需一般对待的;另一类是需要特殊处理的。对仅需一般对待的信息资产采用基本风险评估方法,对需要特殊处理的信息资产采用详细的风险评估方法。两者的结合可将组织机构的费用和资源用于最需要的地方。但该方法也有其自身的缺点,如在对高风险信息系统的鉴别存在错误时,会导致不精确的结果,这将使得对该组织机构的某些重要信息资产的保护失去效果。

风险评估主要依赖于所采用的系统环境、使用信息的商业目的、商业信息和系统的性质等。

4. 确定管制目标和选择管制措施

管制目标的确定和管制措施的选择的基本原则是费用不高于风险所造成的损失。应注意一些风险的后果是无法用金钱来衡量的(如商誉损失等)。由于信息安全是一个动态的系统工程,组织机构应实时对选择的管制目标和管制措施进行校验和调整,以适应情况的变

化,使对组织机构信息资产的保护有效、经济且合理。

5. 准备信息安全适用性声明

信息安全适用性声明记录了组织机构内相关的风险管制目标,及针对每一类风险所采取的对应管制措施。信息安全适用性声明的准备,一方面是为了向组织机构内的员工声明对信息安全面对的风险应当具有的态度,在更大程度上是为了向外界表明组织机构的态度和作为,以表明组织机构已经全面、系统地审视了组织机构的信息安全系统,并将所有必须管制的风险控制在能够被接受的范围内。

1.3.2 信息安全管理体系的实施和运行

信息安全管理体制的规范建立和有效运行是实现信息安全保障的有效手段。

信息安全管理体系建立之后,经过审核与批准并发布实施,信息安全管理体系即进入运行阶段。

在运行期间,要在实践中体验 ISMS 的充分性、适用性和有效性。特别是在初期阶段,组织应加强管理力度,通过实施 ISMS 手册、程序、作业指导书等体系文件,以及教育培训计划、风险处理计划等,评价控制措施的有效性,充分发挥体系本身的各项职能,及时发现存在的问题,找出问题的根源,采取纠正措施,并按照控制程序对体系进行更改,以达到进一步完善 ISMS 的目的。

在实施 ISMS 的过程中,必须充分考虑各种因素,如宣传贯彻、实施监督、考核评审、信息反馈与及时改进等,还要考虑实施的培训费、报名费等各项费用,以及解决员工工作习惯的冲突和不同机构、部门之间的协调等问题,应该做到以下工作:

(1) 做好动员宣传。在实施 ISMS 的前期应召开全体员工会议,由上层管理者做宣传动员,承诺对组织中实施 ISMS 的支持,带头执行 ISMS 的有关规定,并明确提出对各级员工信息安全的职责要求。

(2) 实施培训和安全意识教育计划。ISMS 文件的培训是体系运行的首要任务,培训工作的好坏直接影响体系运行的结果。组织应通过恰当的方式,对全体员工实施各种层次的培训,内容包括信息安全意识、信息安全知识与技能及 ISMS 运行程序等,以确保有关 ISMS 职责的人员具有相应的执行能力。这些方式包括:确定从事影响 ISMS 工作的人员所必要的能力;提供培训或采取其他措施(如聘用有能力的人员)以满足这些需求;评价所采取的措施的有效性;保持教育、培训、技能、经历和资格的记录。

(3) 指定实施风险处置计划。为管理信息安全风险,制定风险处置计划,以识别适当的管理措施、资源、职责和优先顺序,并实施该计划,以达到已识别的控制目标,包括资金安排、角色和职责的分配等。

(4) 实施所选择的控制措施,并评价其有效性。实施风险分析之后选择的控制措施,以满足控制目标的需要,并确定如何测量所选择的控制措施的有效性,以使得管理者和员工确定控制措施达到既定的控制目标。另外,还要指明如何用这些测量措施来评估控制措施的有效性,以产生可比较的和可再现的结果。

(5) 管理 ISMS 的运行。实施对 ISMS 的运行管理,包括以下内容:①管理 ISMS 的资源;②对有关体系运行的信息进行收集、分析、传递、反馈、处理、归档等管理;③建立信息反馈与信息安全协调机制,对异常信息反馈和处理,对出现的体系设计不周、项目不全等问

题加以改进，完善并保证体系的持续正常运行；④实施能够迅速检测安全事件和响应安全事故的程序以及其他控制措施等。

（6）保持 ISMS 的持续有效。ISMS 毕竟只是提供一些原则性的建议，如何将这些建议与组织自身状况结合起来，构架符合实际情况的 ISMS，并保证其有效运行，才是真正具有挑战性的工作。

（7）组织可以通过 ISMS 的监视和定期的审核来验证 ISMS 的有效性，并对发现的问题采取有效的纠正措施并验证其实施效果。ISMS 的运行环境不可能一成不变，当组织的信息系统、组织结构等发生重大改变时，应根据风险评估的结果对 ISMS 进行适当的调整。

1.3.3 信息安全管理体系的监视和评审

1. 信息安全管理体系的监视

信息安全管理体系的监视和评审能够识别出与 ISMS 要求不符合的事项，进而识别出不符合发生和潜在不符合发生的原因，并提出需实施的应对措施。这个过程是 ISMS 的 PDCA 过程的“C”处置阶段，组织应在此阶段做以下工作：

（1）执行监视、评审规程和其他控制措施，以达到以下目的：迅速检测过程运行结果中的错误；迅速识别试图的和得逞的安全违规及事故；使管理者能够确定分配给人员的安全活动或通过信息技术实施的安全活动是否如期执行；通过使用指示器等，帮助检测安全事件并预防安全事故；确定解决安全违规的措施是否有效等。

（2）在考虑安全审核结果、事件、有效性测量结果、所有相关方的建议和反馈的基础上，定期评审 ISMS 的有效性，包括满足 ISMS 方针和目标，以及安全控制措施的评审。

（3）测量控制措施的有效性以验证安全要求是否被满足。

（4）定期进行风险评估的评审，以及对残余风险和已确定的可接受的风险级别进行评审，并且要考虑各方面的变化，如组织情况、技术情况、业务目标和过程、已识别的威胁、已实施的控制措施的有效性、外部事态，如法律法规环境的变更、合同义务的变更和社会环境的变更等。

（5）定期进行 ISMS 内部审核和管理评审。

2. 信息安全管理体系评审

（1）编制评审计划。根据信息安全管理经理提出的要求，由信息安全主管部门拟定体系评审计划，报信息安全管理论坛批准后由主管部门提前分发并通知参加评审人员。

（2）准备评审资料。信息安全主管部门组织有关部门按照评审计划的要求准备体系评审输入所要求的各方面评审资料。评审资料应尽可能充分、全面，由信息安全管理经理向信息安全管理论坛提交信息安全管理体系运行情况报告。

（3）召开评审会议。信息安全管理论坛进行管理评审，评审会议应采用开放的形式，充分听取与体系有关的各方面的意见与建议，由信息安全主管部门记录评审会议结果并编制评审报告。

（4）评审报告分发与保存。评审报告由信息安全管理经理审核、信息安全管理论坛批准，并分发给参加评审的人员和相关部门。评审记录及报告由主管部门按照规定的保存期限予以保存并归档。

（5）评审后要求。对于评审报告中有关决议和措施要求（包括预防和纠正措施），责任

部门应在规定的时间内予以实施，信息安全主管部门应对实施的结果进行验证。

1.3.4　信息安全管理体系的保持和改进

组织建立、实施和保持信息安全管理体系的目的是不断改进组织的信息安全管理绩效，降低安全风险。保护组织关键的信息资产，保持组织商务可持续发展。不断对信息安全管理现状进行评审与审核是持续改进信息安全绩效的有效手段和途径，持续改进是对一个或几个安全管理区域内对风险的程度所采取的改进措施。因为组织信息系统所处的内外部环境是不断变化的，组织信息资产所面临的风险也是一个变数，要想将风险控制在组织可以接受的水平，持续改进是组织必须坚持的信息安全管理原则。

体系评审正是通过对信息安全方针、控制目标和方式的有效性及有关的信息安全管理状况进行评审，寻找并确定改进的机会。经过分析造成不符合的原因，制定改进的纠正和预防措施，进而实施并验证纠正或预防措施的有效性。有效纠正措施的实施又常常促使信息安全方针、控制目标、控制方式、体系文件的更改，从而获得更好的信息安全管理绩效。体系评审正是为改进创造契机，实现持续改进的过程。

组织应采取措施，消除不合格的、与 ISMS 要求不符合的因素，以防止问题再次发生。纠正措施应形成文件，并规定以下方面的要求：

（1）识别在实施和运行 ISMS 过程中的不符合因素。

（2）确定这些不符合因素产生的原因。

（3）对确保这些不符合不再发生所需的措施进行评价。

（4）确定和实施所需要的纠正措施，并记录结果。

（5）评审所采取的纠正措施。

组织应针对潜在的和未来的不合格因素确定预防措施，以防止其发生。所采取的预防措施应与潜在问题的影响程度相适应。预防措施应形成文件，并规定以下方面的要求：

（1）识别潜在的不符合因素的原因。

（2）对预防这些不符合因素发生所需的措施进行评价。

（3）确定和实施所需要的预防措施，并记录结果。

（4）评审所采取的预防措施。

（5）识别发生变化的风险，并通过关注变化显著的风险来识别预防措施的要求。

（6）应根据风险评估的结果来确定预防措施的优先级。

1.4　本章小结

信息安全管理概述部分，主要介绍了信息安全的概念、信息安全的管理以及基于风险的信息安全。信息安全是通过各种计算机、网络和密钥技术，保证在各种系统和网络中传输、交换和存储的信息的机密性、完整性和真实性。信息安全管理是组织中为了完成信息安全目标，针对信息系统，遵循安全策略，按照规定的程序，运用恰当的方法，而进行的规划、组织、指导、协调和控制等活动。风险评估是信息安全管理的基础，没有风险评估，信息安全管理体系的建立就没有依据。

信息安全管理体系部分，详细介绍了信息安全管理体系的相关概念，主要有信息安全管

理体系的框架、信息安全管理体系的过程方法要求以及信息安全管理控制措施要求。

信息安全管理体系建立部分，围绕着建立信息安全管理体系的流程进行了详细的讲解。在信息安全管理体系的规划和建立阶段，首先需要定义信息安全政策，其次定义 ISMS 的范围，然后进行信息安全风险评估，确定管制目标和选择管制措施，最后准备信息安全适用性声明。信息安全管理体系建立完成之后，需要实施和运行，在实施 ISMS 的过程中，必须充分考虑各种因素，如宣传贯彻、实施监督、考核评审、信息反馈与及时改进等。而信息安全管理体系的监督和评审能够识别出与 ISMS 要求不符合的事项，进而识别出不符合发生和潜在不符合发生的原因，并提出需要实施的应对措施。最后，需要对信息安全管理体系进行保持和改进。

第 2 章　信息安全风险管理

现代风险管理理论产生于西方资本主义国家，它是为制定有效的经济发展战略和市场竞争战略而创造的理论、方法和措施，由于风险管理理论的广泛适用性，现已应用于各国社会与经济发展、国家建设、国家安全、公共安全和信息安全诸多领域。管理理论应用于信息安全领域始于 20 世纪 60 年代。此后，信息安全风险管理的实践和理论的发展经过了初级阶段和初步成熟的阶段，最后走向最后一个阶段，即全球化阶段。信息安全风险管理理论来源于信息安全管理实践，信息安全风险管理上存在的问题只能靠信息安全实践来解决。

导入语：本章讲述了信息安全管理相关知识，讲述了信息安全风险管理相关工作内容以及相关定义和风险定义相关方法以及风险管理目标和风险管理的两种方法及其比较，最后一节讲的是风险评估。

考核目标：熟悉并掌握风险相关术语和信息安全风险管理中的 6 个步骤，定量与定性分析方法以及风险评估相关内容。本章主要知识结构如图 2.1 所示。

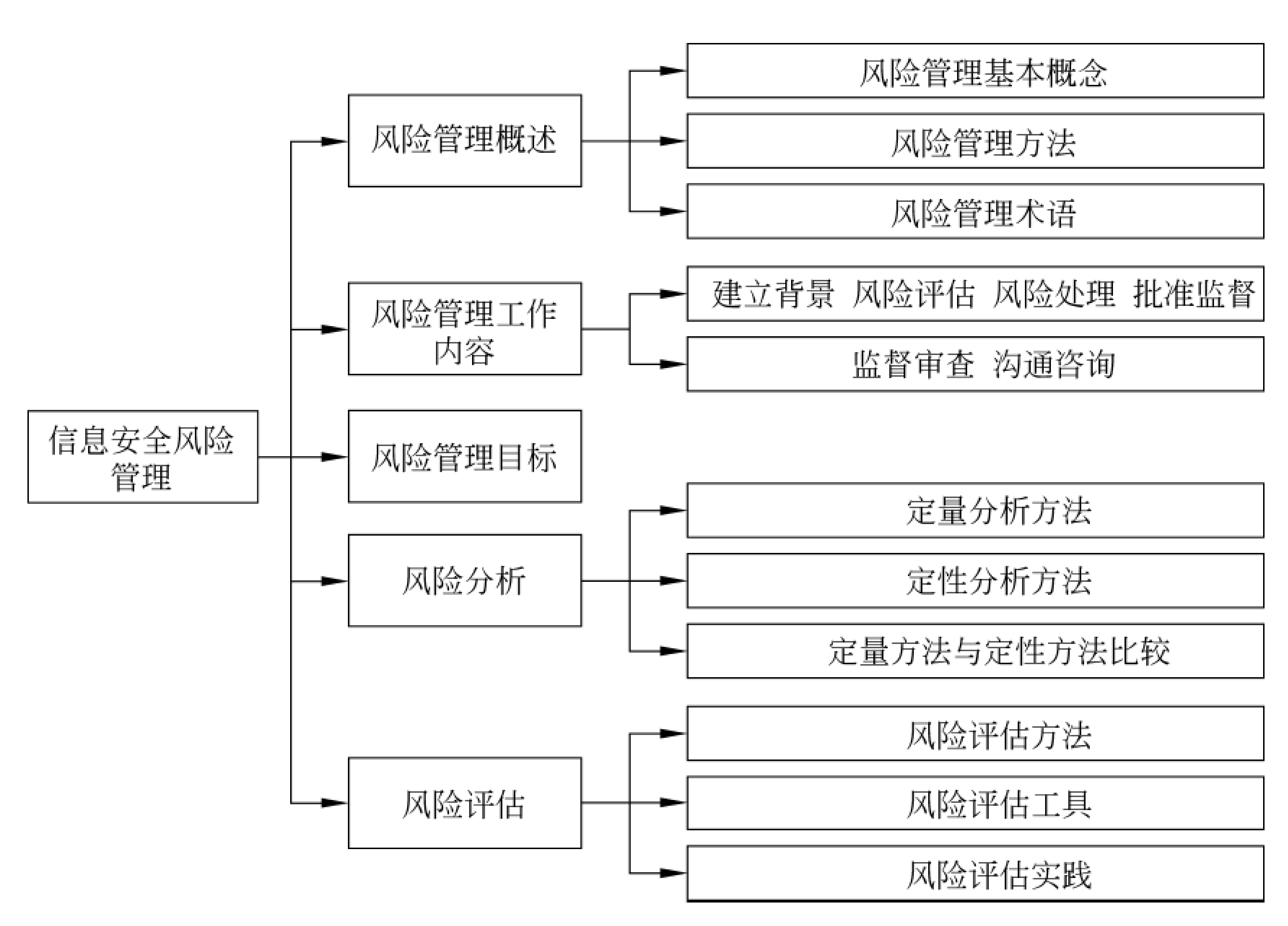


图 2.1　主要知识结构框图

2.1　风险管理概述

2.1.1　风险管理基本概念

当安全投资逐年增加，但看不到收益；当按照国家要求或行业要求开展信息安全工作，但安全事件仍出现。这是因为没有根据风险优先级做安全投资规划，没有抓住主要矛盾，导

致有限资金的有效利用率低,没有根据企业自身安全需求部署安全控制措施,没有突出控制高风险。这就需要风险管理方式,信息安全风险和事件不可能完全避免,没有绝对的安全。信息安全是高技术的对抗,有别于传统安全,呈现扩散速度快、难控制等特点,因此管理信息安全必须以风险管理的方式,关键在于如何控制、化解和规避风险,而不是完全消除风险。而好的风险管理过程可以让机构以最具有成本效益的方式运行,并且使已知的风险维持在可接受的水平。而且好的风险管理过程使组织可以用一种一致的、条理清晰的方式来组织有限的资源并确定优先级,更好地管理风险。而不是将宝贵的资源用于解决所有可能的风险。

管理风险是了解风险和控制风险,风险管理是一个持续的 PDCA 管理过程。信息安全风险管理是识别、控制、消除或最小化可能影响系统资源的不确定因素的过程。也可以认为是在组织机构内部识别、优化、管理风险,使风险降低到可接受水平的过程。

通用风险管理是指如何在一个肯定有风险的环境里把风险减至最低的管理过程。风险管理包括对风险的量度、评估和应变策略。理想的风险管理,是排好一连串优先次序的过程,使引致最大损失及最可能发生的事情优先处理,而相对风险较低的事情则押后处理。

传统上,安全风险管理的方法有两种:前瞻性方法和反应性方法,其各有优缺点。确定某一风险的优先级也有两种不同的方法:定性安全风险管理和定量安全风险管理。

2.1.2 风险管理方法

很多组织通过响应一个相对较小的安全事件而引入安全风险管理。但无论最初的事件是什么,随着越来越多安全有关的问题出现并开始影响业务,很多组织对响应一个接一个的危机感到灰心丧气。他们需要替代方法,即一种能减少首次安全事件的方法。有效管理风险的组织发展了各种前瞻性的方法,但此方法也只是解决方案的一部分。

1. 前瞻性风险管理和反应性风险管理

反应性方法:当一个安全事件发生时,很多 IT 专业人员感到唯一可行的就是遏制情形,指出发生的是什么事情,并尽可能地修复受影响的系统。反应性方法可以是一种已经被利用并转化为安全事件的安全风险的有效技术响应,使反应性方法具有一定程度的严密性,可以帮助所有类型的组织更好地利用他们的资源。

前瞻性方法:与反应性方法相比,前瞻性安全风险管理有很多优点。与等待坏事情发生然后做出反应不同,前瞻性风险管理极大地降低坏事情发生的可能性。

2. 风险管理最佳实践

前瞻性风险管理和反应性风险管理二者相结合才是最佳风险管理方法。例如,流行性感冒是一种致命的呼吸道疾病,美国每年都会有数以百万计的感染者。这些感染者中,至少有 100 000 人必须入院治疗,并且约有 36 000 人死亡。你可能会选择通过等待以确定自己是否受到感染,如果确实受到感染,则采用服药治疗这种方式来治疗疾病。此外,也可以选择在流行性感冒病发季节开始之前接种疫苗。

2.1.3 风险管理术语

在使用风险管理术语时,应该参照中华人民共和国国家标准。

风险管理相关术语有资产、威胁源、威胁、脆弱性、控制措施、可能性、影响、风险、残余风

险及风险评估等。

1. 资产

资产(Asset)是任何对组织有价值的东西,是要保护的对象。资产以多种形式存在(多种分类方法)。

(1) 物理的(如计算设备、网络设备和存储介质等)和逻辑的(如体系结构、通信协议、计算程序和数据文件等)。

(2) 有形的(如机房、设备和人员等)和无形的(如品牌、信心和名誉等)。

(3) 静态的(如设施和规程等)和动态的(如人员和过程等)。

(4) 技术的(如计算机硬件、软件和固件等)和管理的(如业务目标、战略、策略、规程、过程、计划和人员等)等。

2. 威胁

威胁(Threat)是可能导致信息安全事故和组织信息资产损失的活动,威胁源采取恰当的威胁方式才可能引发风险。威胁可以通过威胁主体、资源、动机、途径等多种属性来刻画。

威胁通常有操作失误、滥用授权、行为抵赖、身份假冒、口令攻击、密钥分析等。

3. 脆弱性

脆弱性(Vulnerability)是指与信息资产有关的弱点或安全隐患,是造成风险的内因,脆弱性本身并不对资产构成危害,但是在一定条件得到满足时,脆弱性会被威胁源利用恰当的威胁方式对信息资产造成危害。

脆弱性通常有系统程序代码缺陷、系统设备安全配置错误、系统操作流程有缺陷及维护人员安全意识不足等。

4. 控制措施

控制措施(Countermeasure,Safeguard,Control)是根据安全需求部署,防范威胁和降低风险的措施。

控制措施通常有部署防火墙、入侵检测、审计系统、测试环节、操作审批环节、应急体系。

5. 可能性

可能性(Likelihood, Probability)是指威胁源利用脆弱性造成不良后果的可能性。

例如,脆弱性只有国家级测试人员采用专业工具才能利用,发生不良后果的可能性很小。系统存在漏洞,但只在与互联网物理隔离的局域网运行,发生的可能性较小。互联网公开漏洞且有相应的测试工具,发生不良后果的可能性很大。

6. 影响

影响(Impact,loss)是指威胁源利用脆弱性造成不良后果。

例如,国家级网站被黑客控制,这会对国家造成极其严重的影响,银行门户网站和内部核心系统受到攻击,银行会遭受巨大损失,互联网骨干路由器被攻破,这会对互联网造成极大影响,甚至影响人们的正常上网。

7. 风险

风险(Risk)是指事件发生的不确定性,是指威胁源采用恰当的威胁方式利用脆弱性造成不良后果。风险管理中的风险种类有很多,如纯粹风险、投机风险、财产风险、责任风险、人生风险、信用风险、环境风险、职业风险、自然风险、巨灾风险、社会风险、政治风险、经济风险、税收风险及法规风险。

8. 残余风险

残余风险(Residutal Risk)是指采取了安全措施后,信息系统仍然可能存在的风险。有些残余风险是在综合考虑了安全成本与效益后不去控制的风险。残余风险应受到密切监视,它可能会在将来诱发新的安全事件。

9. 风险评估

信息安全风险评估就是从风险管理角度,运用科学的方法和手段,系统地分析信息系统所面临的威胁及其存在的脆弱性,评估安全事件一旦发生可能造成的危害程度,提出有针对性的抵御威胁的防护对策和整改措施;为防范和化解信息安全风险,将风险控制在可接受的水平,从而最大限度地为信息安全提供科学依据。

10. 信息安全风险术语之间的关系

威胁源采用恰当的威胁方式利用脆弱性造成风险,造成的风险破坏资产,从而造成不良影响,控制措施直接影响威胁源,从而控制不良影响。

2.2 风险管理工作内容

信息安全风险管理包括建立背景、风险评估、风险处理、审核批准、监控与审查和沟通与咨询 6 个方面的内容。建立背景、风险评估、风险处理和审核批准是信息安全管理的 4 个步骤,监控与审查和沟通与咨询则贯穿于这 4 个基本步骤中。

第一步是建立背景,根据要保护系统的业务目标和特性,确定风险管理对象。第二步是风险评估,针对确定的风险管理对象所面临的风险进行识别、分析和评价。第三步是风险处理,依据风险评估的结果,选择和实施合适的安全措施。第四步的审核批准,包括审核和批准两个部分:审核是指通过审查、测试、评审等手段,检验风险评估和风险控制的结果是否满足信息系统的安全要求;批准是指机构的决策层依据审核的结果,做出是否认可的决定。当受保护系统的业务目标和特性发生变化或面临新的风险时,需要再次进入上述 4 个步骤,形成新的依次循环。因此,建立背景、风险评估、风险处理和审核批准构成了螺旋式上升的循环,使得受保护系统在自身和环境的变化中能够不断应对新的安全需求和风险。

监控与审查为上述 4 个步骤进行监控审查。监控是监视和控制,一是监视和控制风险管理过程,即过程质量管理,以保证上述 4 个过程的有效性;二是分析和平衡成本效益及成本效益管理,以保证上述 4 个步骤的成本有效性。审查时跟踪受保护系统自身或所处环境的变化,以保证上述 4 个步骤的结果有效性。监控和审查依据当前步骤的监控和审查结果,控制上述 4 个步骤的主循环,形成许多局部循环。也就是说,当前步骤的监控和审查结果通过时进入下一个步骤;否则继续当前步骤或退到前面的适当步骤。由此,保证主循环中各步骤的有效性。

沟通与咨询为上述 4 个步骤相关人员提供沟通和咨询,沟通是为上述参与人员提供交流途径,以保持他们之间的协调一致,共同实现安全目标。咨询是为上述过程所有相关人员提供学习途径,以提高它们的风险意识和知识,配合实现安全目标。

2.2.1 建立背景

背景建立是信息安全风险管理的第一步,确定风险管理的对象和范围,确立实施风险管

理的准备,进行相关信息的调查和分析。建立背景是为了明确信息安全风险管理的范围和对象,以及对象的特性和安全要求。机构的使命、业务、组织结构、管理制度和技术平台以及国家、地区、行业的相关政策、法律、法规和标准都是对象确立的必要依据。

建立背景的过程包括风险管理准备,信息系统调查,信息系统分析和信息安全分析 4 个阶段。在信息安全风险管理的过程中,对象确立过程是一次信息安全风险管理主循环的起始,风险评估提供输入,监控与审查和沟通与咨询贯穿其 4 个阶段,背景建立流程如图 2.2 所示。

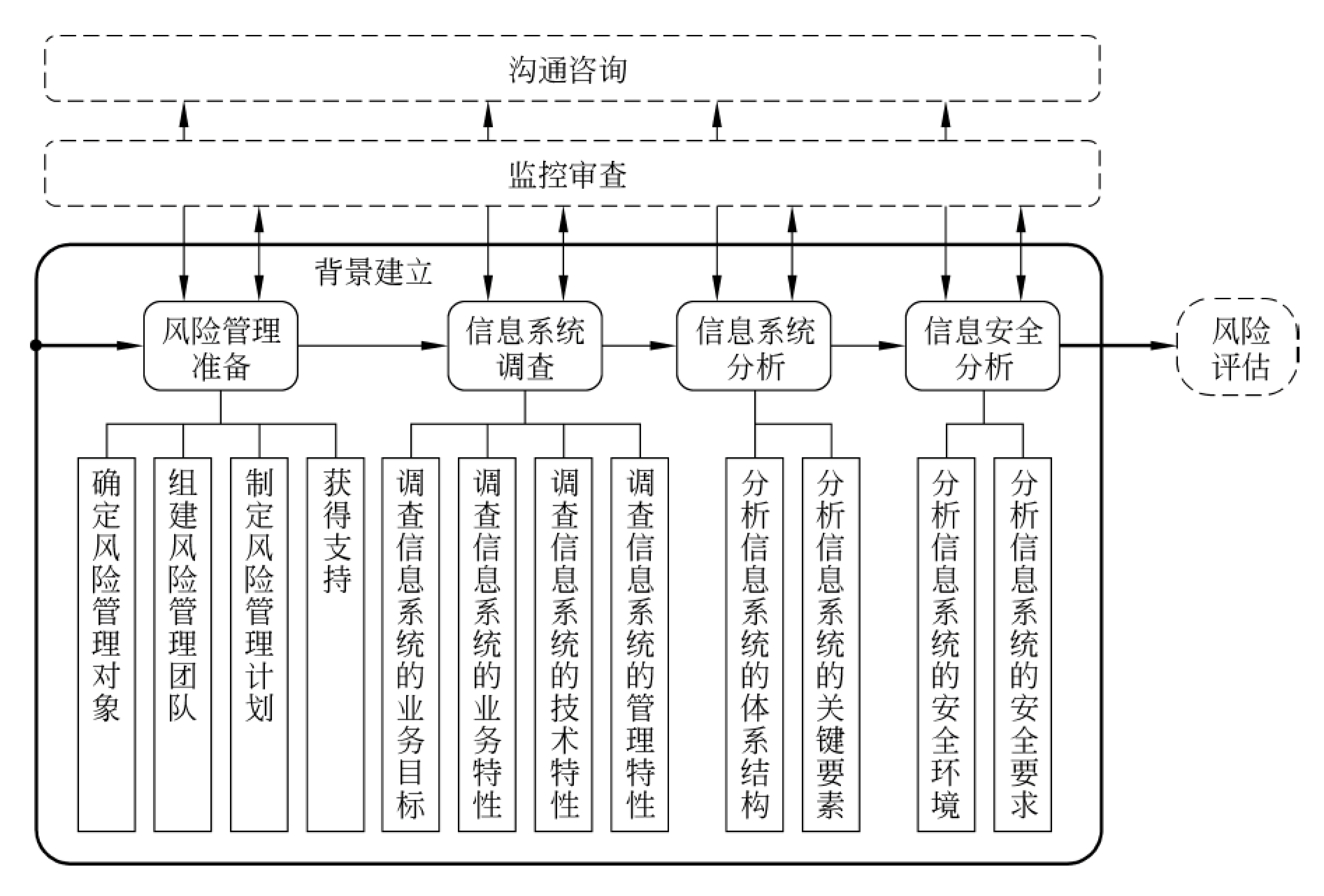


图 2.2 背景建立流程

2.2.2 风险评估

风险评估是信息安全管理的第二步,针对确立的风险管理对象所面临的风险进行识别、分析和评价。

安全风险是一种潜在的、负面的东西,处于未发生的状态。与之相对应,安全事件是一种显在的、负面的东西,处于已经发生的状态。风险是事件发生的前提,事件是在一定条件下由风险演变而来。

风险的构成包括 5 个方面:起源、方式、途径、受体和后果。起源是威胁的发起方,叫做威胁源;方式是威胁源所采取的手段,叫做威胁行为;途径是威胁源所利用的薄弱环节,叫做脆弱性或漏洞;受体是资产;后果是影响。

风险评估分成 4 个步骤。

(1) 风险分析准备。制定风险评估方案、选择评估方法。

(2) 风险要素识别。发现系统存在的威胁、脆弱性和控制措施。

(3) 风险分析。判断风险发生的可能性和影响的程度。

(4) 风险结果判定。综合分析结果判定风险等级。

风险评估过程包括风险评估准备、风险因素识别、风险程度分析和风险等级评价 4 个阶段。在信息安全风险管理过程中,接受对象的输出,为风险控制提供输入,监控与审查和沟

通与咨询贯穿 4 个阶段,如图 2.3 所示。

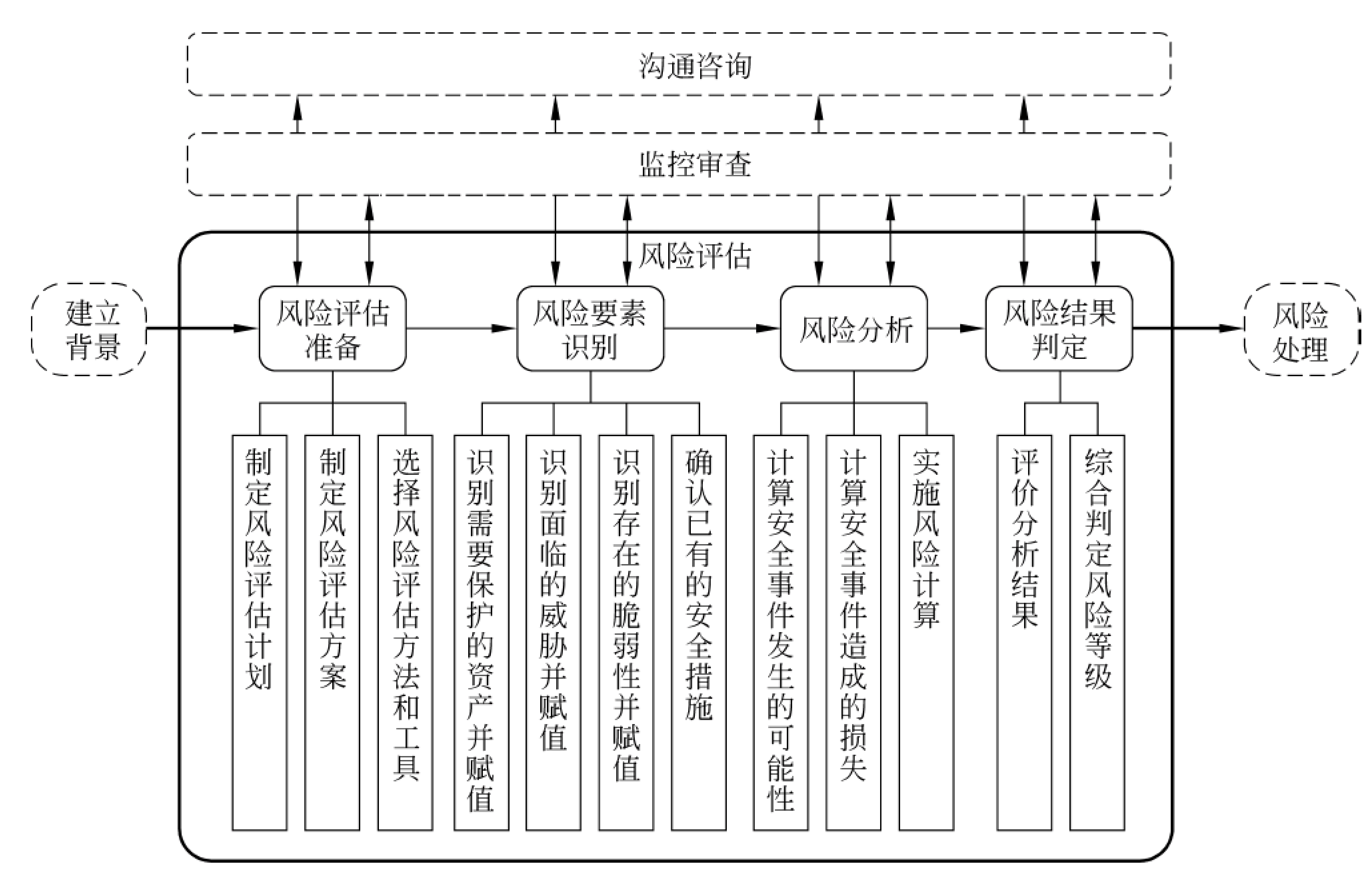


图 2.3　风险评估流程

2.2.3　风险处理

风险处理是信息安全管理的第三步,依据风险评估的结果,选择、实施及使用安全措施。风险处理是为了将风险始终控制在可接受范围内。

风险处理也分成 4 个步骤。

(1) 现存风险判断。判断信息系统中哪些风险可以接受,哪些不可以。

(2) 处理目标确认。不可接受的风险需要控制到怎样的程度。

(3) 处理措施选择。选择风险处理方式,确定风险控制措施。

(4) 处理措施实施。制定具体安全方案,部署控制措施。

风险处理的过程包括风险判断、控制目标确立、控制措施选择和控制措施实施 4 个阶段。在信息安全风险管理过程中,接受风险评估的输出,为审核批准提供输入,监控与审查和沟通与咨询贯穿其 4 个阶段,如图 2.4 所示。

常用的 4 类风险处置方法分别是降低风险、转移风险、规避风险及接受风险。

1. 降低风险

通过对面临风险的资产采取保护措施来降低风险。

首先应当考虑的风险处置措施,通常在安全投入小于负面影响价值的情况下采用。

保护措施可以从构成风险的 5 个方面(即威胁源、威胁行为、脆弱性、资产和影响)来降低风险。

降低风险的具体办法分成 3 种:减少威胁源、降低威胁能力及减少脆弱性。

(1) 减少威胁源。

采用法律的手段制裁计算机犯罪,发挥法律的威慑作用,从而有效遏制威胁源的动机。

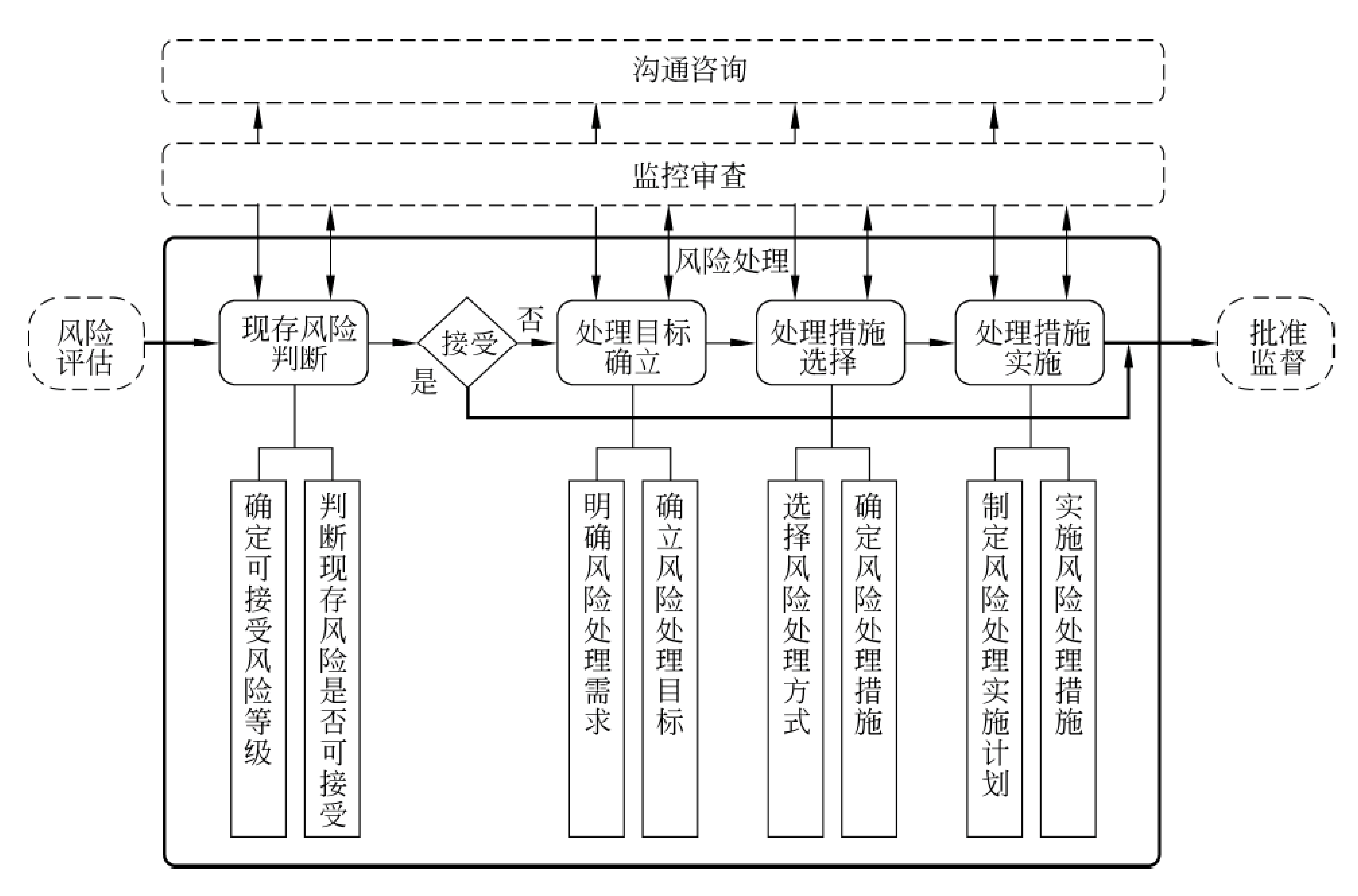


图 2.4　风险处理流程

（2）降低威胁能力。

采取身份认证措施，从而抵制身份假冒这种威胁行为的能力。

（3）减少脆弱性。

及时给系统打补丁，关闭无用的网络服务端口，从而减少系统的脆弱性，降低被利用的可能性。

2. 转移风险

通过将面临风险的资产或其价值转移到更安全的地方来避免或降低风险。

通常只有当风险不能被降低或避免且被第三方（被转嫁方）接受时才被采用。一般用于那些低概率、但一旦风险发生时会对组织产生重大影响的风险。

转移风险的具体做法分成如下两种：

（1）在本机构不具备足够的安全保障的技术能力时，将信息系统的技术体系（即信息载体部分）外包给满足安全保障要求的第三方机构，从而避免技术风险。

（2）通过给昂贵的设备上保险，将设备损失的风险转移给保险公司，从而降低资产价值的损失。

3. 规避风险

通过不使用面临风险的资产来避免风险。例如：

（1）在没有足够安全保障的信息系统中，不处理特别敏感的信息，从而防止敏感信息的泄漏。

（2）对于只处理内部业务的信息系统，不使用互联网，从而避免外部的有害入侵和不良攻击。

通常在风险的损失无法接受，又难以通过控制措施降低风险的情况下采用规避风险。

4. 接受风险

接受风险是对风险不采取进一步的处理措施,接受风险可能带来的结果。

很多人倾向于选择风险转移对策,但不是所有风险都是可转移的,或者说将这些风险转移是不经济的。对于这些风险就不得不自留。此外,在某些情况下,自留一部分风险也是合理的。例如,工程保险如果采用的是全额保险,那么保险费可能非常高,而如果规定一个合适的免赔额,则可以大大降低保险费。

接受风险不意味着不闻不问,需要对风险态势变化进行持续的监控,一旦发展为无法接受的风险就要进一步采取措施。

2.2.4 批准监督

1. 批准监督的概念

批准监督是信息安全风险管理的第四个步骤,包括批准和持续监督两部分。批准是指机构的决策层依据风险评估和风险处理的结果是否满足信息系统的安全要求,做出是否认可风险管理活动的决定。持续监督是指检查机构及其信息系统以及信息安全相关的环境有无变化,监督变化因素是否有可能引入新的安全隐患并影响到信息安全系统的安全保障级别。

批准应由机构内部或更高层的主管机构的决策层来执行。持续监督通常由机构内部管理层和执行层完成,必要时也可以委托支持层取得外部专业机构提供支持,这主要取决于信息系统的性质和机构自身的专业能力。

2. 批准监督的原则

对风险评估和风险处理的结果的批准和持续监督,不是仅依据相关标准进行僵化的对比过程,而是紧紧围绕着信息系统所承载的业务,通过对业务重要性和业务遭受损失后所带来的影响来开展相关工作。批准监督的依据有两个:一是信息系统的参与风险是可以接受的;二是安全措施满足信息管理系统当前业务的安全需要。

3. 批准监督的过程

批准监督的过程包括批准申请、批准处理和持续监督 3 个阶段。在信息安全风险管理过程中,接受风险管理输出是一次信息安全风险管理活动的终点,监控与审查和沟通与咨询贯穿其 3 个阶段,批准监督的过程如图 2.5 所示。

第一阶段:批准申请包括提交批准申请和受理批准申请。

(1) 提交批准申请。申请者填写批准申请书之后,连同批准材料一起提交给批准机构。批准材料内容包括管理过程中输出的文档、软件和硬件等结果。批准申请书内容包括批准的范围、对象和期望以及申请者的基本信息和签字等。批准机构由在信息系统和信息安全风险管理的决策层中负责重大决定的主管者构成。

(2) 受理批准申请。批准机构接收批准申请书和审核结论报告并审查通过之后,返回批准受理回执、批准受理同意受理、材料补充以及批准机构的名称和签章等。

第二阶段:批准处理包括审阅批准材料和做出批准决定。

(1) 审阅批准材料。批准机构依据机构的使命和信息系统的安全的要求报告,按照批准的原则、规定和程序,对批准材料进行审阅,与相关人员进行讨论和沟通,为批准决定做准备。

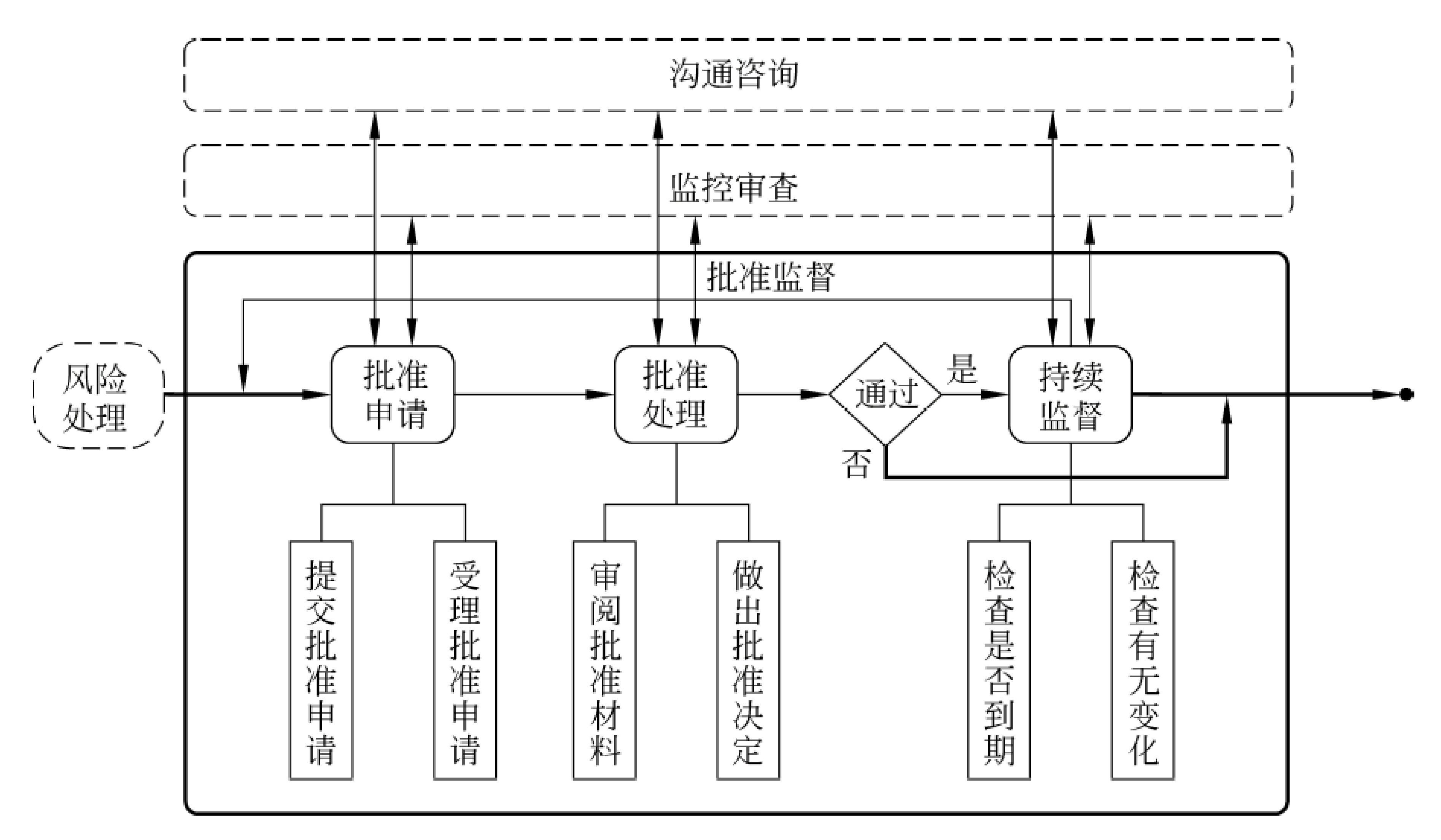


图 2.5　批准监督的过程

（2）做出批准决定。批准机构按照批准的原则、规定和程序，判断信息系统安全要求是否得到满足，机构的信息安全保障级别是否达到所需要的等级，依次作出决定，形成批准决定书，交付申请者。

第三阶段：持续监督的工作包括检查是否到期和检查有无变化。

（1）检查是否到期。如果批准监督有效期到期则发出批准到期通知书。批准有效到期需要重新开始批准监督的过程。

（2）检查有无变化：一是检查机构信息系统有无变化；二是检查信息安全相关的环境有无变化。如果有变化分别给出机构变化因素的描述报告和环境变化因素报告。

2.2.5　监控审查

1. 监控审查的概念

监控审查对背景建立、风险评估、风险处理和批准监督进行审查。监控是监视和控制：一是监视和控制风险管理过程，即过程质量管理，以保证过程的有效性；二是分析和平衡成本效益，即成本效益管理，以保证成本的有效性。

2. 监督审查的意义

监控与审查可以及时发现已经出现或即将出现的变化、偏差和延误等问题，并采取适当的措施进行控制和纠正，从而减少因此造成的损失，保证信息安全风险管理主循环的有效性。

3. 监督审查的过程

监督审查的过程贯穿于整个信息安全管理过程，并输出相应的监控审查记录，如图 2.6 所示。监控审查记录内容包括监控和审查的范围、对象、时间、过程、结果和措施等。

建立背景
风险评估
风险处理
批准监督
监控审查
背景建立的监控与审查记录
风险评估的监控与审查记录
风险处理的监控与审查记录
批准监督的监控与审查记录

图 2.6　监督审查流程

2.2.6 沟通咨询

1. 沟通咨询的概念

沟通与咨询为信息安全风险管理主循环的 4 个步骤，即确立背景、风险评估、风险处理和审核批准中的相关人员提供沟通与咨询。沟通是为直接参与人员提供交流途径，以保持他们之间协调一致，共同实现安全目标。咨询是为所有相关人员提供学习途径，以提高他们的风险意识、知识和技能，配合实现安全目标。

2. 沟通与咨询的意义

为保证信息安全风险管理活动顺利和有效地进行，相关人员行动的协调和一致以及相关知识和技能的熟练掌握是十分关键的因素。通过畅通的交流和充分的沟通，保持行动的协调和一致；通过有效的培训和方便咨询，保证行动者有足够的知识和技能，这就是沟通和咨询的意义所在。

3. 沟通和咨询的目标

（1）与决策层沟通，以得到他们的理解和支持。

（2）与管理层和执行层沟通，以得到他们的理解和协作。

（3）与支持层沟通，以得到他们的了解和支持。

（4）与用户层沟通，以得到他们的了解和配合。

4. 沟通和咨询的过程

沟通咨询的过程贯穿信息安全风险管理的建立背景、风险评估、风险处理和审核批准这 4 个基本步骤，并分别输出相应的沟通咨询记录，如图 2.7 所示。沟通与咨询内容包括沟通和咨询的范围、对象、时间和结果等。

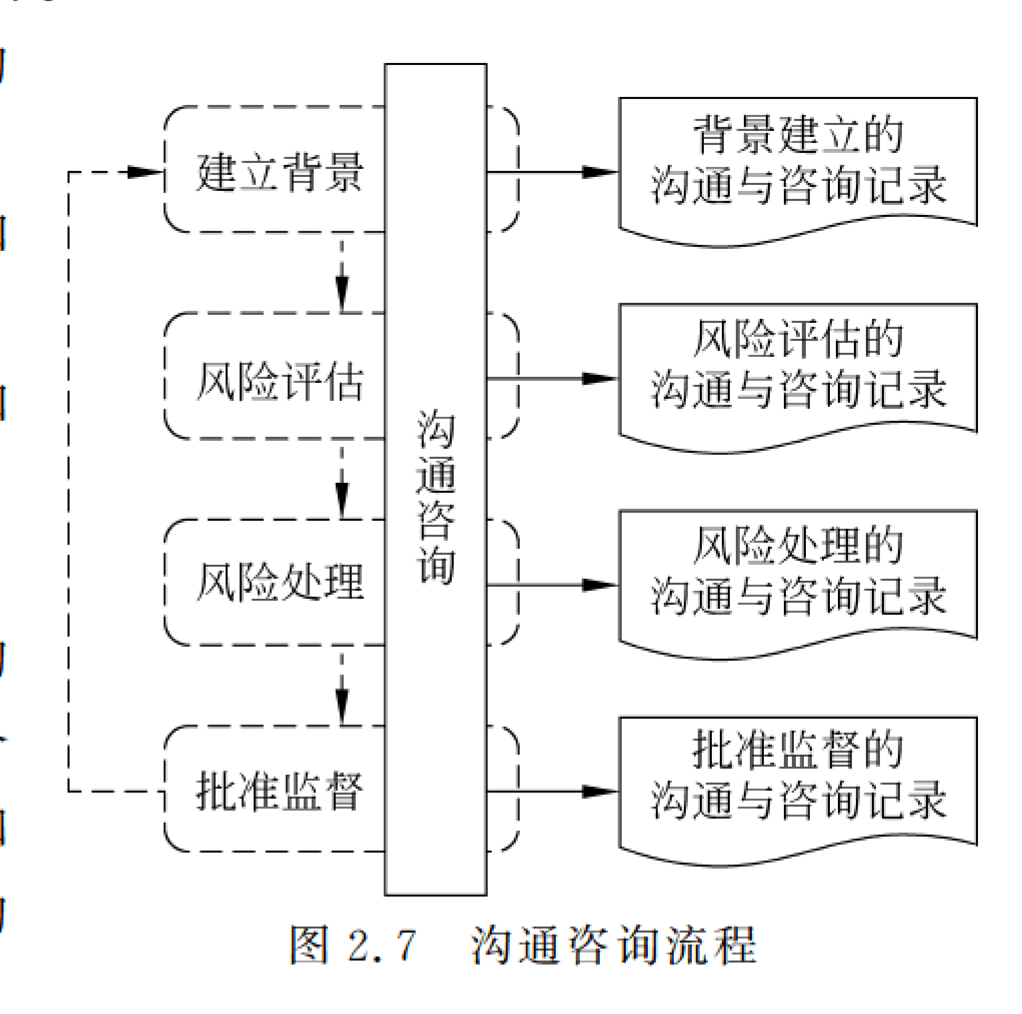


图 2.7　沟通咨询流程

2.3 风险管理目标

信息安全风险管理是信息安全保障工作中的一项基础性工作，是需要贯穿信息系统生命周期、持续进行的工作。分成 5 个步骤，即规划、设计、实施、运维和废弃。

2.3.1 规划

规划阶段风险评估的目的是识别系统的使命，用以支撑系统安全需求及安全战略等。规划阶段的评估应能够描述信息系统建成后对现有业务模式的作用，包括技术、管理等方面，并根据其作用确定系统建设应达到的安全目标。

本阶段评估中，资产、脆弱性不需要识别，威胁应根据未来系统的应用对象、应用环境、业务状况、操作要求等方面进行分析。评估应着重以下几方面：

（1）是否从组织上依据相关规则确立信息系统整体规划，是否与业务战略相一致，并得

到最高管理者的认可。

（2）整体规划中是否明确系统开发的组织、业务变更的管理、开发优先级。

（3）整体规划中是否考虑系统的威胁、环境和制定总体的安全方针。

（4）描述信息系统预期使用的信息，包括预期的应用、信息资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等。

（5）描述所有与信息系统安全相关的运行环境，包括物理和人员的安全配置以及明确相关的法规、组织安全政策、习惯、专门技术和知识等。

规划阶段的评估结果应体现在信息系统整体规划或项目建议书中。

明确信息系统安全建设的目的，对信息系统安全建设实现的可能性进行分析论证并设计出总体安全规划方案。为了保证安全目标的实现，需要对信息系统规划阶段中可能引入安全风险的环节进行风险管理，从而降低在项目后期处理相同安全风险所带来的高额成本，如表 2.1 所示。

表 2.1　规划的风险管理活动及其过程

序号	风险管理活动	所处风险管理过程	序号	风险管理活动	所处风险管理过程
1	明确安全总体方针	建立背景	3	风险评估准则达成一致	风险评估
2	安全需求分析	建立背景	4	安全实现论证分析	风险处理、批准监督

2.3.2　设计

设计阶段的风险评估需要根据规划阶段所明确的系统运行环境、资产重要程度，提出安全功能需求。设计阶段的风险评估结果应对设计开发计划中所提供的安全功能符合性进行判断，作为采购过程风险控制的依据。

本阶段评估中，应详细评估设计开发计划中对系统面临威胁的描述、将使用的具体设备、软件等资产的列表以及这些资产的安全功能需求。评估对象是开发设计计划和安全需求分析，对部分将二者合一的系统建设方案，则直接评审系统建设方案。

对开发设计计划的评估包括以下内容：

（1）设计开发计划是否符合系统建设规划，并得到最高管理者的认可。

（2）是否对系统建设后面临的威胁进行了分析。重点分析来自物理环境和自然的威胁，由于内、外部入侵等造成的威胁。

（3）设计开发计划是否明确目的、业务对象、费用、效果等各项内容。

（4）是否采取了一定的手段应对系统可能的故障。

（5）对设计或者原型中的技术实现以及人员、组织管理等各方面的脆弱性进行评估，包括设计过程中的管理脆弱性和技术平台固有的脆弱性。

系统分析及需求定义的评估要点包括以下内容：

（1）是否符合规划阶段的安全目标，并基于威胁的分析，制定系统建设的总体安全策略。

（2）是否考虑可能随着其他系统介入而产生的风险。

（3）信息系统建成后可能对业务、管理体制及各种规程等的影响。

（4）是否根据开发的规模、时间及系统的特点选择开发方法，并根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型。

（5）系统的性能是否满足潜在用户需求，并考虑到峰值的影响，是否在技术上考虑了满足系统性能要求的方法。

（6）数据库是否根据业务需要进行设计。

（7）设计活动中所采用的安全控制措施、安全技术保障手段对风险结果的影响。在安全需求变更和设计变更后，也需要重复这项评估。

在设计信息系统的实现结构和实施方案时，在技术的选择、配合、管理等众多的环节均容易引入安全风险，因此对关键的环节应提出必要的安全要求，并有针对性地进行安全风险管理。信息系统设计阶段的信息安全风险管理如表 2.2 所示。

表 2.2 信息系统设计阶段的信息安全风险管理

序　　号	风险管理活动	所处风险管理过程
1	设计方案分析论证	建立背景、风险评估
2	安全技术选择	风险处理
3	安全产品选择	风险处理
4	自开发软件设计风险处理	风险处理

2.3.3 实施

实施阶段风险评估的目的是根据系统安全需求和运行环境对系统开发实施过程进行风险识别，并对系统建成后的安全功能进行验证。根据设计阶段分析的威胁和建立的安全控制措施，在实施及验收时进行质量控制。

基于设计阶段的资产列表、安全措施以及评估开发过程中对上述要求的保障，实施阶段应对规划阶段的安全威胁作进一步细分，同时评估安全措施的实现程度，从而确定上述安全措施能否抵御现有威胁、脆弱性的影响。实施阶段风险评估包括开发与获取阶段、实施交付阶段两部分评估。

开发与获取阶段的具体评估要点包括如下：

（1）法律、政策、适用标准和指导方针。评估直接或间接影响信息安全需求的特定法律；评估政府政策、国际或国家标准对系统安全需求的影响。

（2）系统的功能需要。安全需求是否有效地支持系统的功能。

（3）成本效益风险。系统的资产、威胁和弱点，以确定在符合相关法律、政策、标准和系统功能需要下最合适的防范措施。

（4）评估保证级别。指明系统建设后应进行怎样的测试和检查，从而确定是否满足项目建设、实施规范。

（5）评估系统开发/获取阶段的安全活动包括系统安全开发的内容、开发过程的监视、安全问题的防范、需求更改的响应以及监视外来的威胁。

实施交付阶段的具体评估要点包括如下：

（1）根据实际建成的系统，详细分析其面临的威胁。

（2）根据系统建设目标和安全需求，对系统的安全功能进行验收测试；评价安全功能能否抵御安全威胁。

（3）评估是否建立了与整体安全策略一致的组织管理制度。

（4）对系统实现的风险控制效果与预期设计的符合性进行判断，如存在较大的不符合，应重新进行系统安全策略的设计与调整。信息系统实施阶段的风险管理如表 2.3 所示。

表 2.3　信息系统实施阶段的风险管理

序号	风险管理活动	所处风险管理过程	序号	风险管理活动	所处风险管理过程
1	安全测试	风险评估	3	人员培训	风险处理
2	检查与配置	风险处理	4	授权系统运行	批准监督

2.3.4　运维

运维阶段风险评估的目的是了解和控制运行过程中的信息系统安全风险，是一种较为全面的风险评估。评估内容包括对真实运行的信息系统、资产、威胁、脆弱性等各方面。

（1）资产评估。对真实环境下较为细致的评估，包括实施阶段采购的软硬件资产、系统运行过程中生成的信息资产、相关的人员与服务等。本阶段资产识别是前期资产识别的补充与增加。

（2）威胁评估。真实环境中的威胁分析，应全面地评估威胁的可能性和影响程度。对非故意威胁产生安全事件的评估可以参照事故发生率；对故意威胁主要由评估人员就威胁的各个影响因素做出专业判断；同时考虑已有控制措施。

（3）脆弱性评估。这是全面的脆弱性评估。包括运行环境下物理、网络、系统、应用、安全保障设备、管理的脆弱性。对于技术的脆弱性评估采取核查、扫描、案例验证、渗透性测试的方式验证脆弱性；对安全保障设备脆弱性评估时考虑安全功能的实现情况和安全措施本身的脆弱性。对于管理脆弱性采取文档、记录核查进行验证。

（4）风险计算。根据本标准的相关方法，对主要资产的风险进行定性或定量的风险分析，描述不同资产的风险高低状况。

运维阶段的风险评估应定期执行；当组织的业务流程、系统状况发生重大变化时，也应进行风险评估。重大变更时包括以下变更（但不限于）：

（1）增加新的应用或应用发生较大变更。

（2）网络结构和连接状况发生较大变更。

（3）技术平台大规模的更新。

（4）系统扩容或改造后进行。

（5）发生重大安全事件后，或基于某些运行记录怀疑将发生重大安全事件。

（6）组织结构发生重大变动对系统产生影响。

信息系统运行维护阶段的风险管理，如表 2.4 所示。

表 2.4　信息系统运行维护阶段的风险管理

序号	风险管理活动	所处风险管理过程	序号	风险管理活动	所处风险管理过程
1	安全运行和管理	风险评估、风险处理	3	风险再评估	风险评估、风险处理
2	变更管理	风险评估、风险处理	4	定期重新审批	批准监督

2.3.5　废弃

废弃阶段风险评估的目的是确保硬件和软件等资产及残留信息得到了适当的废弃处置,并确保系统更新过程在一个安全、系统化的状态下完成。

本阶段应重点对废弃资产对组织的影响进行分析,并根据不同的影响制定不同的处理方式。对由于系统废弃可能带来的新的威胁进行分析,并改进新系统或管理模式。对废弃资产的处理过程应在有效的监督之下实施,同时对废弃的执行人员进行安全教育。

维护工作的技术人员和管理人员均应该参与此阶段的评估。

信息系统废弃阶段的风险管理如表 2.5 所示。

表 2.5　信息系统废弃阶段的风险管理

序号	风险管理活动	所处风险管理过程	序号	风险管理活动	所处风险管理过程
1	确定废弃对象	建立背景	3	废弃过程的风险处理	风险处理
2	废弃对象的风险评估	风险评估	4	废弃后的评审	批准监督

2.4　风险分析

在风险评估的过程中,可以采取多种操作方法,包括基于知识的分析方法、基于模型的分析方法、定量分析和定性分析方法,无论何种方法,共同的目标都是找出信息资产面临的风险及其影响,以及目前安全水平与组织安全需求之间的差距。这里只介绍定量和定性分析方法。

2.4.1　定量分析方法

定量分析方法的思路很明确:对构成风险的各个要素和潜在损失的水平赋予数值或者货币金额,当风险的所有要素(资产价值、威胁频率、弱点利用程度、安全措施的效率和成本等)都被赋值,风险评估的整个过程和结果就可以被量化了。简单地说,定量分析方法就是试图从数字上对安全风险进行分析评估的一种方法。定量分析中有以下几个重要的概念。

(1) 评估资产。根据资产价值(AV)清单,计算资产总价值及资产损失对财务的直接和间接影响。

(2) 确定单一预期损失(SLE)。SLE 是指发生一次风险引起的收入损失总额,是分配给单个事件的金额,代表一个具体威胁利用漏洞时将面临的潜在损失(SLE 类似于定性风险分析的影响)。将资产价值与暴露系数相乘(EF)计算出 SLE。暴露系数表示为现实威胁对某个资产造成的损失百分比。

(3) 确定年发生率 ARO。ARO 是一年中风险发生的次数。

(4) 确定年预期损失 ALE。ALE 是不采取任何减轻风险的措施在一年中可能损失的总金额。SLE 乘以 ARO 即可计算出该值。ALE 类似于定量风险分析的相对级别。

假定某公司投资 500 000 美元建了一个网络运营中心,其最大的威胁是火灾,一旦火灾发生,网络运营中心的估计损失程度是 45%。根据消防部门推断,该网络运营中心所在的地区每 5 年会发生一次火灾,于是得出了 ARO 为 0.20 的结果。基于以上数据,该公司网络运营中心的 ALE 将是 45 000 美元。

可以看到,对定量分析来说,有两个指标是最为关键的,一个是事件发生的可能性(可以用 ARO 表示),另一个就是威胁事件可能引起的损失(用 EF 来表示)。从理论上讲,通过定量分析可以对安全风险进行准确的分级,但这有个前提,那就是可供参考的数据指标是准确的,可事实上,在信息系统日益复杂多变的今天,定量分析所依据的数据的可靠性是很难保证的,再加上数据统计缺乏长期性,计算过程又极易出错,这就给分析的细化带来了很大困难,所以,目前的信息安全风险分析,采用定量分析或者纯定量分析方法的已经比较少了。

(5) 确定控制成本。控制成本就是为了规避企业所存在风险的发生而应投入的费用。

(6) 安全投资收益 ROSI,即

(实施控制前的 ALE)-(实施控制后的 ALE)-(年控制成本)=ROSI

2.4.2 定性分析方法

定性分析方法是目前采用最为广泛的一种方法,它带有很强的主观性,往往需要凭借分析者的经验和直觉或者业界的标准和惯例,为风险管理诸要素(资产价值、威胁的可能性、弱点被利用的容易度、现有控制做事的效力等)的大小或高低程度定性分级,如"高"、"中"、"低"三级。

定性分析的操作方法多种多样,包括小组讨论、检查列表、问卷、人员访谈及调查等。定性分析操作起来相对容易,但可能因为操作者经验和直觉偏差而失准。

(1) 后果或影响的定性量度(示例)如表 2.6 所示。

表 2.6 后果或影响的定性量度表

等级	描述	详细情形	等级	描述	详细情形
1	可以忽略	无伤害,低财物损失	4	较大	大伤害,失去生产能力有较大财物损失
2	较小	立即受控制,中等财物损失	5	灾难性	持续能力中断,巨大财物损失
3	中等	受控,高财物损失			

(2) 可能性的定性量度(示例)如表 2.7 所列。

表 2.7 可能性的定性量度

等级	描述	详细情形	等级	描述	详细情形
A	几乎肯定	预期在大多数情况下发生	D	不太可能	在某个时间能够发生
B	很可能	在大多数情况下很可能会发生	E	罕见	仅在例外的情况下可能发生
C	可能	在某个时间可能会发生			

(3) 风险分析矩阵——风险程度,如表 2.8 所示。

表 2.8　风险分析矩阵表

可能性	后果				
	可以忽略 1	较小 2	中等 3	较大 4	灾难性 5
A(几乎肯定)	H	H	E	E	E
B(很可能)	M	H	H	E	E
C(可能)	L	M	H	E	E
D(不太可能)	L	L	M	H	E
E(罕见)	L	L	M	H	H

注:E,极度风险;H,高风险;M,中等风险;L,低风险。

定性分析方法——相乘法:

(1) 计算安全事件发生可能性。

威胁发生频率:威胁 $T_1=1$。

脆弱性严重程度:脆弱性 $V_1=3$。

安全事件发生可能性$=\sqrt{1}\cdot\sqrt{3}$。

(2) 计算安全事件的损失。

资产价值:资产 $A_1=4$。

脆弱性严重程度:脆弱性 $V_1=3$。

计算安全事件的损失,安全事件损失$=\sqrt{3}\cdot\sqrt{4}$。

(3) 计算风险值。

安全事件发生可能性。

安全事件损失。

安全事件风险值$\sqrt{3}\cdot\sqrt{12}=6$。

(4) 确定风险等级,如表 2.9 所示。

表 2.9　风险等级表

风险值	1～5	6～10	11～15	16～20	21～25
风险等级	1	2	3	4	5

2.4.3　定性分析方法与定量分析方法的比较

定性分析与定量分析各有优、缺点,定性分析与定量分析相比较,定性分析的准确性稍好但精确性不够,定量分析则相反;定性分析没有定量分析那样繁多的计算负担,但却要求分析者具备一定的经验和能力;定量分析依赖大量的统计数据,而定性分析没有这方面的要求;定性分析较为主观,定量分析基于客观。此外,定量分析的结果很直观,容易理解,而定性分析的结果则很难有统一的解释。组织可以根据具体的情况来选择定性或定量的分析方法。具体的比较如表 2.10 所示。

表 2.10 定性分析与定量分析优、缺点表

方法	优　　点	缺　　点
定量分析	(1) 按经济影响排列风险优先级;按经济价值排列资产价值 (2) 风险管理的效果以投资回报率衡量 (3) 结果可用因管理而异的术语来表达(如货币值和表达为具体百分比) (4) 随着组织建立数据的历史记录并获得经验,其精确度将随时间的推移而提高	(1) 风险影响值以参与者的主观意见为基础 (2) 取得风险一致意见的过程非常耗时 (3) 计算可能会非常复杂且耗时 (4) 风险结果以财务术语表达,对非技术性人员而言可能难以解释 (5) 流程要求专业技术,因此参与者无法轻松通过流程获得指导
定性分析	(1) 风险排名具有可见性,易于理解 (2) 更容易达成一致意见 (3) 无须量化威胁发生频率 (4) 无须确定资产的财务价值 (5) 更便于不是安全或计算机专家的人员参与	(1) 重要风险之间没有显著区别 (2) 因为没有成本效益分析,很难证明控制措施的投资是合理的 (3) 结果取决于风险管理小组人员的主观判断

2.5 风险评估

信息安全风险管理要依靠风险评估的结果来确定随后的风险控制和审核批准活动。风险评估使得机构能够准确定位风险管理策略、实践和工具,能够将安全活动的重点放在重要问题上,能够选择成本效益合理和适用安全对策。基于风险评估的风险管理方法被实践证明是有效的和实用的,已被广泛应用于各个领域。

风险评估只是为信息安全活动提供一个方向,并不会导致重大的信息安全的改进,不管评估方法有多详细多专业,也只能描述风险状态,而不会改进机构安全状态。机构只有利用评估结果持续地进行改进活动,实现风险有效管理,才能使得机构的安全状态得到改善。评估好坏的价值标准在于其对随后的风险控制和审核批准的指导作用,良好和确切的风险评估是成功的信息安全风险管理的基础。

信息安全风险评估分为自评估、检查评估两种形式。以自评估为主,自评估和检查评估相互结合、互为补充。自评估和检查评估可依托自身技术力量进行,也可委托第三方机构提供技术支持。

2.5.1 评估方法

1. 风险评估的工作形式——自评估

(1) 优点。

更容易达成一致意见,无须量化威胁发生频率,有利于保密、发挥行业和部门内人员的业务特长、降低风险评估的费用以及提高本单位的风险评估能力与信息安全知识。

(2) 缺点。

可能由于缺乏风险评估的专业技能,其结果不够深入、准确;同时,受到组织内部各种因素的影响,其评估结果的客观性易受影响。

(3) 建议方法。

委托风险评估服务技术支持方实施的评估,过程比较规范、评估结果的客观性比较好,

可信程度较高;但由于受到行业知识技能及业务了解的限制,对被评估系统的了解,尤其是在业务方面的特殊要求存在一定的局限。但由于引入第三方本身就是一个风险因素,因此,对其背景与资质、评估过程与结果的保密要求等方面应进行控制。

2. 风险评估的工作形式——检查评估

检查评估是指信息系统上级管理部门组织的或国家有关职能部门依法开展的风险评估。优点:最具权威性,通过行政手段加强信息安全的重要措施。缺点:间隔时间较长,一般是抽样进行,难以贯穿信息系统的生命周期。

2.5.2 风险评估工具

风险评估与管理工具集成了风险评估各类知识和判据的管理信息系统,以规范风险评估的过程和操作方法;或者是用于收集评估所需要的数据和资料,基于专家经验,对输入输出进行模型分析。

系统基础平台风险评估工具主要用于对信息系统的主要部件(如操作系统、数据库系统、网络设备等)的脆弱性进行分析,或实施基于脆弱性的攻击。

风险评估辅助工具实现对数据的采集、现状分析和趋势分析等单项功能,为风险评估各要素的赋值、定级提供依据。

2.5.3 风险评估实践

1. 实施内容——评估准备

风险评估的准备是整个风险评估过程有效性的保证。组织实施风险评估是一种战略性的考虑,其结果将受到组织业务战略、业务流程、安全需求、系统规模和结构等方面的影响。因此,在风险评估实施前,应做到以下几点:

(1)确定风险评估的目标。

风险评估的准备阶段应明确风险评估的目标,为风险评估的过程提供导向。信息系统是重要的资产,其机密性、完整性和可用性对于维持竞争优势、获利能力、法规要求和组织形象是必要的。组织要面对来自内、外部日益增长的安全威胁,信息系统是威胁的主要目标。由于业务信息化程度不断提高,对信息技术的依赖日益增加,一个组织可能出现更多的脆弱性。风险评估的目标是满足组织业务持续发展在安全方面的需要,或符合相关方的要求,或遵守法律法规的规定等。

(2)确定风险评估的范围。

基于风险评估目标确定风险评估范围是完成风险评估的前提。风险评估范围可能是组织全部的信息及与信息处理相关的各类资产、管理机构,也可能是某个独立的系统、关键业务流程、与客户知识产权相关的系统或部门等。

(3)组建适当的评估管理与实施团队。

基于风险评估目标确定风险评估范围是完成风险评估的前提。风险评估范围可能是组织全部的信息及与信息处理相关的各类资产、管理机构,也可能是某个独立的系统、关键业务流程、与客户知识产权相关的系统或部门等。组建适当的风险评估管理与实施团队,以支持整个过程的推进,如成立由管理层、相关业务骨干、IT 技术人员等组成的风险评估小组。评估团队应能够保证风险评估工作的有效开展。

（4）选择与组织相适应的具体的风险判断方法。

选择方法应考虑评估的目的、范围、时间、效果、人员素质等因素来选择具体的风险判断方法，使之能够与组织环境和安全要求相适应。

（5）获得最高管理者对风险评估工作的支持。

上述所有内容确定后应得到组织的最高管理者的支持、批准，并对管理层和技术人员进行传达，应在组织范围就风险评估相关内容进行培训，以明确各有关人员在风险评估中的任务。

2. 实施评估——现场信息获取

实施评估时应该遵循以下几个步骤：

（1）召开现场评估启动会议。

（2）资产识别。资产是具有价值的信息或资源，是安全策略保护的对象。它能够以多种形式存在，有无形的、有形的，有硬件、软件，有文档、代码，也有服务、形象等。机密性、完整性和可用性是评价资产的 3 个安全属性。信息安全风险评估中资产的价值不仅仅以资产的账面价格来衡量，而是由资产在这 3 个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的。安全属性达成程度的不同将使资产具有不同的价值，而资产面临的威胁、存在的脆弱性以及已采取的安全措施都将对资产安全属性的达成程度产生影响。为此，有必要对组织中的资产进行识别。

（3）威胁识别。威胁是一种对组织及其资产构成潜在破坏的可能性因素，是客观存在的。造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和无意两种。环境因素包括自然界不可抗的因素和其他物理因素。威胁作用形式可以是对信息系统直接或间接的攻击，如非授权的泄露、篡改、删除等，在机密性、完整性或可用性等方面造成损害；也可能是偶发的或蓄意的事件。

（4）物理环境脆弱性评估。从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别。

（5）网络脆弱性识别。从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别。

（6）系统脆弱性识别。审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别。

（7）管理脆弱性评估。管理脆弱性评估应该从技术管理和组织管理两个方面开始。从技术管理层面上：物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性。在组织管理层面上应包括安全策略、组织安全、资产分类与控制、人员安全、符合性。

（8）渗透测试。渗透性测试的目的是检测已发现的漏洞是否真正会给系统或网络环境带来威胁。通常渗透性工具与漏洞扫描工具一起使用。

（9）确认现场评估结果。

3. 风险分析

1）风险计算原理

在完成了资产识别、威胁识别、脆弱性识别以及对已有安全措施确认后，将采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性，通过考虑安全事件一旦发生其所作用资产的重要性及脆弱性的严重程度来判断安全事件造成的损失对组织的影响，即

安全风险。本标准给出了风险计算原理，以下面的范式形式化加以说明：

$$风险值=R(A,T,V)=R(L(T,V),F(I_a,V_a))$$

其中，R 表示安全风险计算函数；A 表示资产；T 表示威胁；V 表示脆弱性；I_a 表示安全事件所作用的资产重要程度；V_a 表示脆弱性严重程度；L 表示威胁利用资产的脆弱性导致安全事件发生的可能性；F 表示安全事件发生后产生的损失。有以下 3 个关键计算环节：

（1）计算安全事件发生的可能性。

根据威胁出现频率及脆弱性状况，计算威胁利用脆弱性导致安全事件发生的可能性，即安全事件发生的可能性$=L$(威胁出现频率，脆弱性)$=L(T,V)$在具体评估中，应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（可访问时间、设计和操作知识公开程度等）以及资产吸引力等因素来判断安全事件发生的可能性。

（2）计算安全事件发生后的损失。

根据资产重要程度及脆弱性严重程度，计算安全事件一旦发生后的损失，即安全事件的影响$=F$(资产重要程度，脆弱性严重程度)$=F(I_a,V_a)$部分安全事件的发生造成的影响不仅仅是针对该资产本身，还可能影响业务的连续性；不同安全事件的发生对组织造成的影响也是不一样的。在计算某个安全事件的损失时，应将对组织的影响也考虑在内。

（3）计算风险值。

根据计算出的安全事件发生的可能性以及安全事件的损失，计算风险值，即风险值$=R$(安全事件发生的可能性，安全事件的损失)$=R(L(T,V),F(I_a,V_a))$。评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法，通过构造经验函数，采用矩阵法可形成安全事件发生的可能性与安全事件的损失之间的二维关系；运用相乘法可以将安全事件发生的可能性与安全事件的损失相乘得到风险值。

2）风险结果判定

风险等级划分为 5 级，等级越高，风险越高。评估者应根据所采用的风险计算方法为每个等级设定风险值范围，并对所有风险计算结果进行等级处理，如表 2.11 所示。

表 2.11　风险等级划分

等级	标识	描　　述
5	很高	一旦发生将使系统遭受非常严重的破坏，组织利益受到非常严重的损失
4	高	如果发生将使系统遭受严重的破坏，组织利益受到严重的损失
3	中	发生后将使系统受到较重的破坏，组织利益受到损失
2	低	发生后将使系统受到的破坏程度和利益损失一般
1	很低	即使发生只会使系统受到较小的破坏

4. 风险处置建议

组织应当综合考虑风险控制成本与风险造成的影响，提出一个可接受风险阈值。对某些风险，如果评估值不大于可接受风险阈值，是可接受风险，可保持已有的安全措施；如果评估值大于可接受风险阈值，是不可接受风险，则需要采取安全措施以降低、控制风险。

在不可接受风险选择适当的安全措施后，为确保安全措施的有效性，可进行再评估，以判断实施安全措施后的残余风险是否已经降低到可接受的水平。残余风险的再评估可以依

据本标准提出的风险评估流程进行，也可做适当裁减。某些风险可能在选择了适当的安全措施后仍处于不可接受的风险范围内，应考虑是否接受此风险或进一步增加相应的安全措施。

5. 规避风险工作带来的新风险

在进行风险规避工作的同时也会产生一些其他的新风险，如表 2.12 所示。

表 2.12 新工作带来的风险表

可能属性	影响属性	威胁程度	应对措施
内部信息外泄	保密性	高	评估机构资质、法律保证、评估过程控制（如核心部分不离开用户单位）
评估结果的有效性	可用性	中	评估机构资质、评估人员资质、案例经验
评估结果的准确性	完整性、可用性	中	评估机构资质、评估人员资质、案例经验
占用大量用户时间	可用性	低	成熟、量化的调查模式
安全检测意外中断业务	完整性、可用性	高	人员资质、测试环境、应急计划、恢复演练
安全测试影响正常业务（如网络、主机的可用性）	可用性	高	错开业务高峰、提高检测命中率
渗透测试影响正常业务	可用性	高	人员能力、黑白兼顾、应急预案和演练
其他可能意外原因			应急小组 7×24h 支持

2.6 本章小结

风险管理概述部分主要介绍了风险管理术语、方法、概念等。风险管理的工作内容主要介绍了建立背景、风险评估、风险处理、批准监督、监控与审查和沟通咨询 6 个方面的内容，以及各个过程的概念、意义、过程和目标。风险管理目标主要讲述了信息安全管理的 5 个步骤，即规划、设计、实施、运维和废弃。风险分析主要介绍了两种风险分析方法：定性分析方法和定量分析方法，以及这两种分析方法各自的优、缺点。最后一部分主要讲了风险评估的方法、风险评估的过程以及风险评估实践。

第 3 章　基本信息安全管理

导入语：本章系统地介绍了基本的信息安全管理，从基本概念入手，层层剖析不同的管理层次、不同管理方面的具体内容，并结合管理中所要遵循的原则给出实际例子，使读者更能进一步理解管理中每个步骤的实施办法和实施意义。安全措施管理主要分为基本安全管理措施和重要安全管理过程。而本章则主要对于基本安全管理措施进行重点讲解。本章主要知识结构见图 3.1 所示。

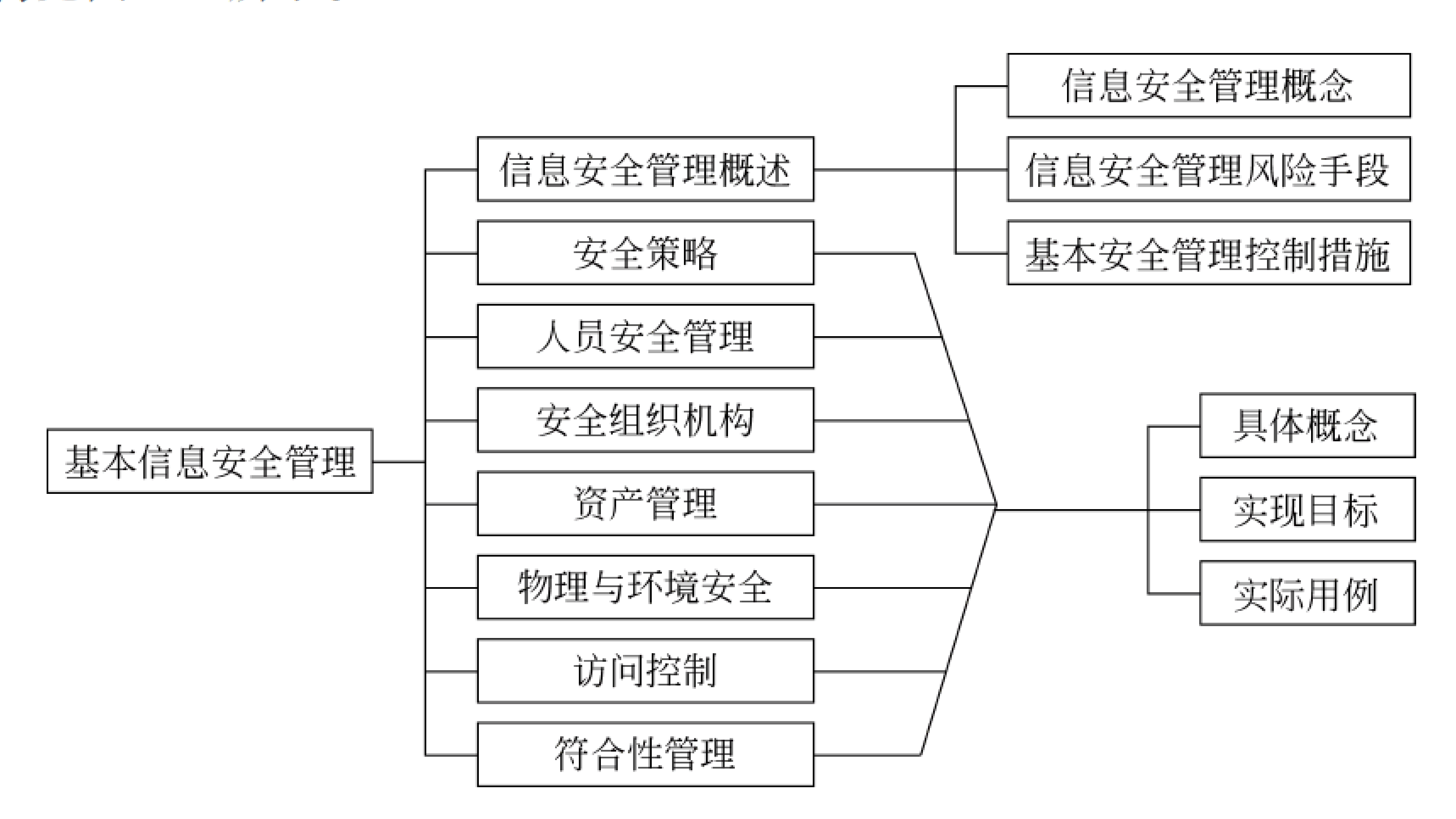


图 3.1　本章主要知识结构框图

考核目标：本章围绕基本信息安全管理，逐节介绍了不同的管理方面。要求读者掌握每节介绍内容的基本概念、实施目标和意义。在理解概念的基础上了解基本信息安全管理的实例，并通过实例再次加深对概念的理解。本章介绍的内容概念性较强，建议读者要把概念文字与实际应用相结合，以便更能深层次地了解基本信息安全管理。

3.1　信息安全管理概述

3.1.1　信息安全管理相关概念

现实世界里大多数安全事件的发生和安全隐患的存在，与其说是技术上的原因，不如说是管理不善造成的，理解并重视管理对于信息安全的关键作用，对于真正实现信息安全目标来说尤其重要。信息安全管理可从 3 个方面进行理解，即何为信息、何为信息安全、何为信息安全管理。

信息是日常生活中再熟悉不过的词语。日常的口头交流的内容属于信息，通过手机等通信工具传达的内容也属于信息。信息可以是看得见、摸得到的实物，也可以是一种无形但却同样具有意义的消息，而在本章节中讨论的则是后者。这种信息是一种资产，像其他重要的业务资产一样，对组织具有价值，因此需要妥善保护。

日常生活中的信息交流以及和亲朋好友之间进行轻松休闲的信息交换时，信息安全并不是一个引起人们重视的问题。但当在计算机或者网络上保存了学习或者工作中特别重要的信息时就必须要考虑到信息安全这一方面。这就要求根据信息安全的特性制定相应的策略去保护信息。

信息安全主要指信息的保密性、完整性和可用性的保持。即指通过采用计算机软硬件技术、网络技术、密钥技术等安全技术和各种组织管理措施，来保护信息在其生命周期内的产生、传输、交换、处理和存储的各个环节中，信息的保密性、完整性和可用性不被破坏。

信息安全管理是通过维护信息的保密性、完整性和可用性，来管理和保护组织所有的信息资产的一项体制；是组织中用于指导和管理各种控制信息安全风险的一组相互协调的活动，有效的信息安全管理要尽量做到在有限的成本下，保证安全风险控制在可接受的范围。

其作为组织完整的管理体系中一个重要环节，它构成了信息安全具有能动性的部分，是指导和控制组织的关于信息安全风险的相互协调的活动，其针对对象就是组织的信息资产。

3.1.2 信息安全管理风险的手段

信息安全管理风险的手段有多种，面对不同的情况要采取不同的应对措施。有时采用其中一种方法即可奏效，而有时需要多种方法结合使用方能达到最理想的效果。常用的3种方法如下。

1. 降低风险

降低风险即是通过面临风险的资产采取保护措施来降低风险。降低风险是当遇到风险时首先应考虑风险处置措施，通常在安全投入小于负面影响价值的情况下采用。所采取的保护措施可以从构成风险的5个方面（即威胁源、威胁行为、脆弱性、资产和影响）来降低风险。

当采用降低风险这种手段来管理风险时需要进行以下操作：

（1）采用法律的手段制裁计算机犯罪，发挥法律的威慑作用，从而有效遏制威胁源的动机，即减少威胁源。

（2）采取身份认证措施，从而抵制身份假冒这种威胁行为的能力，即降低威胁能力。

（3）及时给系统打补丁，关闭无用的网络服务端口，从而减少系统的脆弱性，降低被利用的可能性，即减少脆弱性。

（4）采用各种防护措施，建立资产的安全域，从而保证资产不受侵犯，其价值得到保持，即防护财产。

（5）采取容灾备份、应急响应和业务连续计划等措施，从而减少安全事件造成的影响程度，即降低负面影响。

2. 避免风险

通过不使用面临风险的资产来避免风险。例如，在没有足够安全保障的信息系统中，不处理特别敏感的信息，从而防止敏感信息的泄露；对于只处理内部业务的信息系统，不使用互联网，从而避免外部的非法入侵和不良攻击。

避免风险这种管理手段是试图防止漏洞被利用的风险控制策略。通常在风险的损失无法接受，又难以控制措施降低风险的情况下才会使用。通常有3种常用的方法。

（1）应用政策。这种方法允许管理人员颁布特定的后续步骤。例如，如果机构需要更

严格地控制密码的使用，就应该执行一项政策，要求所有的 IT 系统都使用密码。注意，仅有政策是不够的，高效的管理人员总是使政策与教育培训，或者技术的应用，或者二者协调起来。

（2）教育培训。必须使员工了解政策。另外，新技术通常需要培训。如果希望员工的行为比较安全、能控制，认识、培训以及教育就是必不可少的。

（3）应用技术。在信息安全中，通常需要技术解决方案来确保减少风险。如密码可用于大多数现代的操作系统，但一些系统管理员可能没有配置系统，同样可以使用密码。如果政策要求使用密码，管理员也意识到它的必要性，并参加了培训，这个控制技术就会得到成功的使用。

3. 转移风险

转移风险即是通过将面临风险的资产或其价值转移到更安全的地方来避免或降低风险。通常只有当风险不能被降低或避免且被第三方（被转嫁方）接收时才被采用。一般用于那些低概率、但一旦风险发生时会对组织产生重大影响的风险。

当选择转移风险这种手段时，可以采取以下做法：

（1）在本机构不具备足够的安全保障的技术能力时，将信息系统的技术体系（即信息载体部分）外包给满足安全保障要求的第三方机构，从而避免技术风险。

（2）通过给昂贵的设备上保险，将设备损失的风险转移给保险公司，从而降低资产价值的损失。

这样，机构就可以将管理复杂系统的风险转嫁给对处理这些风险有经验的另一个机构。使用专业合同的一个好处是提供商对灾难恢复负责，并通过服务级别协定，来保证服务器和网站的可用性。但是外包并非不存在风险。信息资产的所有者、IT 管理人员和信息安全组要保证外包合同中的灾难恢复要求足够多，并在进行恢复工作前得到满足。如果外包商没有履行合同条款，结果就可能比预计的要糟糕得多。

4. 接受风险

接受风险是选择对风险不采取进一步的处理措施，接受风险可能带来的后果。接受风险用于那些在采取了降低风险和避免风险措施后，出于实际和经济方面的原因，只要组织进行运营，就必然存在并必须接受的风险。

但是，接受风险并不意味着不闻不问，需要对风险态势变化进行持续的监控，一旦发展为无法接受的风险就要采取进一步的措施。而要采取进一步的有效措施只有在进行以下工作之后才可以进行：

（1）确定了风险等级。

（2）评估了攻击的可能性。

（3）估计了攻击带来的潜在破坏。

（4）进行了全面的成本效益分析。

（5）评估了使用每种控制的可行性。

（6）认定了某些功能、服务、信息或者资产不值得保护。

如果机构中每个已识别的漏洞都通过接受策略来处理，就说明该机构没有能力采取安全措施，总体上对安全是漠不关心的。机构不能将无知当作一种理由，并以不知道有责任保护员工、客户的信息为借口来避免被起诉。管理人员不能认为，如果他们对信息不加以保

护,攻击者就会觉得那些不被保护的信息并不重要,从而对机构的系统不采取攻击。

3.1.3 基本安全管理控制措施内容

1. 控制措施

控制措施就是管理风险的方法。该方法能为企业目标提供合理保证,并能预防、检查和纠正风险的作用。它们可以是行政、技术、管理、法律等方面的措施。

2. 控制措施的分类

1)预防性控制措施

(1)在问题发生前发现潜在问题,并作出纠正。

(2)仅雇佣胜任的人员。

(3)职责分工。

(4)使用访问控制软件,只允许授权用户访问敏感文件。

2)检查性控制

(1)检查控制发生的错误、疏漏或蓄意行为。

(2)生产作业中设置检查点。

(3)网络通信过程中的 Echo 控制。

(4)内部审计。

3)纠正性控制

(1)减少危害影响,修复检查性控制发现的问题。

(2)意外处理计划。

(3)备份流程。

(4)恢复运营流程。

3.2 安全策略

3.2.1 安全策略的概念

充分了解组织业务特征是设计安全管理策略的前提,只有了解组织业务特征,才能发现并分析组织业务所处的风险环境,并在此基础上提出合理的、与组织业务目标相一致的安全保障措施,并给出该措施所需要的技术和控制方法,从而制定出有效的安全管理策略和程序。

对组织业务的了解包括对其业务内容、性质、目标及其价值进行分析。在信息安全中,业务一般是以资产形式表现,它包括信息/数据、软/硬件、无形资产、人员及其能力等。安全风险管理理论认为,对业务资产的适度保护对业务的成功至关重要。要实现对业务资产的有效保护,必须要对资产有很清晰的了解。

通过对组织文化及员工状况的了解,掌握组织中员工的安全意识、心理状况和行为状况,为制定合理的安全政策打下基础。

要制定一套好的安全管理策略,必须与决策层进行有效沟通,并得到组织高层领导的支持与承诺,这有 3 个作用:一是制定的安全管理策略与组织的业务目标一致;二是制定的安

全方针政策、控制措施可以在组织的上上下下得到有效的贯彻；三是可以得到有效的资源保证，比如在制定安全策略时，必要的资金与人力资源的支持及跨部门之间的协调工作都必须由高层管理人员来推动。

另外，要确定信息安全整体目标及其所涉及的范围，描述信息安全宏观需求和预期达到的目标。一个典型的目标是：通过防止安全事故和最小化事故影响，保证业务持续性，并最小化业务损失，为企业实现业务目标提供保障。

确定安全管理策略要涉及的范围，组织需要根据自己的实际情况，可以在整个组织范围内或者在个别部门或领域制定安全管理策略，这需要与组织实施的信息安全管理体系范围结合起来考虑。

根据风险评估与选择安全控制的结果，起草拟定安全策略，安全策略要尽可能地涵盖所有的风险和控制，没有涉及的内容要说明原因，根据具体的风险和控制来决定制定什么样的策略。

信息安全策略是一个组织解决信息安全问题最重要的步骤，也是这个组织整个信息安全体系的基础。信息安全不是天然的需求，而是经历了信息损失之后才有的需求，所以管理对于信息安全是必不可少的。一个组织最主要的管理文件就是信息安全策略，信息安全策略明确规定组织需要保护什么，为什么需要保护和由谁进行保护。没有合理的信息安全策略，再好的信息安全专家和安全工具也没有价值。一个组织的信息安全策略可以反映出这个组织对现实安全威胁和未来安全风险的预期，也可反映出组织内部业务人员和技术人员对安全风险的认识与应对。信息安全策略是陈述管理者的管理意图，说明信息安全工作目标和原则的文件。从本质上来说是描述组织具有哪些重要信息资产，并说明这些信息资产如何被保护的一个计划。

例如，有单位领导说："听说信息安全工作很重要，可是我不知道对于我们单位来说到底有多重要，也不知道究竟有哪些信息是需要保护的。据说作为管理人员要把个人计算机的登录口令设置好，怎么设置才符合要求呢？"

上面的例子都是在公司企业中常见的问题，这样的问题就要从安全策略的角度切入，从中寻找答案。

3.2.2 安全策略的目标

信息安全策略是指为信息安全提供与业务需求和法律法规相一致的管理指示及支持。安全策略应该做到以下几点：

(1) 对信息安全加以定义。

(2) 陈述管理层的意图。

(3) 分派责任。

(4) 约定信息安全管理的范围。

(5) 对特定的原则、标准和遵守要求进行说明。

(6) 对报告可疑安全事件的过程进行说明。

(7) 定义用以维护策略的复查过程。

3.2.3 安全策略的实例

企业信息安全策略：它为信息安全部门定下了基础，并确定整个机构信息安全的大环境。该策略是顺应IT战略性计划而开发的，一般由首席信息安全官草拟，再由首席信息官或首席执行官支持和签署通过。

基于问题的安全策略：在使用技术时(如电子邮件、因特网)所定义的可被接受的行为规则。

基于系统的策略：它实际上是采用技术或管理措施来控制设备的配置。例如，访问控制列表就是这种策略，它定义了对某个特殊设备的访问权限。表3.1给出了一些常用信息安全策略的示例。

表3.1 一些常用信息安全策略

政策名称	内容简介
可接受的使用策略(AUP)	为了保护组织信息资产，定义组织内部的设备、计算服务、安全方法的使用规范，这些规范是员工必须遵守的，组织可以接受的
物理安全	保护信息处理设施、数据、人员免受物理入侵、盗窃、火灾、水灾和其他自然灾害的影响
网络设备安全	定义组织信息系统环境中网络设备最小安全需求，包括各类交换机、路由器等
服务器安全	定义组织信息系统环境中服务器最小安全需求，包括各类应用系统服务器、数据库服务器、事务处理服务器等
信息分类	对信息资产要有详细的记录与分类并做适当的价值与重要性评估，以便采用相对应的安全措施来保护其机密性、完整性与可用性
信息保密	定义组织中的哪些敏感信息必须进行加密保护，并采用什么样的加密算法
用户账号及口令	定义用户账号及口令的规范，及采用、保护和改变口令的标准
远程访问	定义外部用户通过网络连接，访问组织内部资源的规则与要求
反病毒	定义组织中预防病毒与检测病毒的技术与管理措施
防火墙及入侵检测	定义组织中预防与检测外部非法入侵所采取的技术与管理措施
员工使用E-mail	定义员工使用E-mail的有关规定
员工使用Internet	定义组织使用Internet的有关规定
第三方使用组织的Extranet	定义外部第三方(如客户、厂商、合作伙伴)连接组织内部网，访问资源时必须遵守的规定
外购评审	对组织的外购信息设施进行安全评审，并定义最小安全要求
使用软件	对在组织内使用商业与非商业软件的版权与许可证的要求
软件获得与开发	定义组织在进行软件开发或外购软件所要遵守的安全规定
安全事件的调查与响应	对于组织中发生的任何安全事件，员工都要及时报告给相关信息安全部门与人员，安全事件要得到及时的调查与处置
灾难恢复与业务持续性计划	定义灾难发生时应对灾难的措施与程序，相关人员的职责，联系办法等
风险评估	为信息安全人员识别、评估和控制风险而提供授权和定义需求
信息系统审计性	为信息安全人员实施风险评估和审计活动，提供授权和定义需求，以保证信息与资源的完整性与法律法规的符合性，并监测系统和用户的活动

3.3 人员安全管理

3.3.1 人员安全管理的概念

随着 Internet 技术的发展和网络知识的日益普及,人们对信息的获取从来没有像今天这样便利和迫切,伴随而来的是对信息系统安全的威胁,这种威胁不仅是对某一个单位、社团、组织的,还可能发展成为对国家主权、机密的威胁,因此保护信息系统的安全是当务之急。

信息系统的建设和运用离不开具体实施操作的工作人员,他们不仅是计算机信息系统建设和应用的主体,同时也是安全管理的对象。因此在整个信息安全管理中,人员安全管理是至关重要的。要确保信息系统的安全,必须加强人员的安全管理。

管理的实现必须依赖于组织行为,做好信息安全工作也要建立与系统规模、重要程度相适应的安全组织机构。

各级计算机安全管理组织的职责和主要任务是管好与系统有关的人员,包括其思想品德、职业道德和业务素质等。这对于系统直接经营单位而言尤为重要。计算机安全管理组织的目标是管好计算机资产,即计算机信息系统资源和信息资源安全。这是一个崭新的公共安全工作领域,按以往惯例,必须使安全工作组织机构不能隶属于计算机运行或应用部门,而应当由安全负责人负责安全组织的具体工作,直接对单位主要领导以及公安主管部门负责。这也是建立安全组织的基本要求。

人员管理要落实在人员各阶段的活动中。

(1) 雇佣(上岗)前。明确人员遵守安全规章制度、执行特定的信息安全工作、报告安全事件或潜在风险的责任。对担任敏感和重要岗位的人员要考察其身份、学历和技术背景、工作履历和以往的违法违规记录。要在合同或专门的协议中,明确其信息安全职责。

(2) 雇佣中。保证其充分了解所在岗位的信息安全角色和职责;有针对性地进行信息安全意识教育和技能培训;采取及时有效的惩戒措施。

(3) 离职。终止职责,通知相关人员人事变化,明确离职后仍需遵守的责任规定;归还资产,保证离职人员归还软件、计算机、存储设备、文件和其他设备;撤销访问权限,撤销用户名、门禁卡、密钥、数字证书等。

3.3.2 人员安全管理的目标

各种各样的防护措施均离不开人的掌握和控制,因此系统的安全最终是由人来控制的。安全离不开工作人员的审查、控制和管理,要通过制定、执行和实施各种管理制度以及各种安全保护条例来实现,因而在安全组织中人员的职能划分尤为重要。

为防止品质不良或不具备一定技能的人员进入组织,或不具备一定资格条件的员工被安排在关键或重要岗位,组织应明确雇佣员工的条件和考核评价的方法与程序,减少因雇佣员工而产生的安全风险。

(1) 雇佣前。确保员工、合同方和第三方用户了解他们的责任并适合于他们所考虑的

角色，减少盗窃、滥用或设施误用的风险。

（2）雇佣中。确保所有的员工、合同方和第三方用户了解信息安全威胁和相关事宜、他们的责任和义务，并在他们的日常工作中支持组织的信息安全方针，减少人为错误的风险。

（3）解聘和变更。确保员工、合同方和第三方用户离开组织或变更雇佣关系时以一种有序的方式进行。

人员安全管理的终极目标就是要实现组织的安全管理，从最基本的人员管理做起，才能更加有效地管理一个组织，才能保证一个组织健康正常的运行。

3.3.3 人员安全管理的实例

员工缺乏基本的安全意识，特别是一些业务人员等，没有进行统一的、系统的安全培训和学习的机会。由于员工对发生安全问题后造成的后果不负任何责任，从而也就不能有效地督促员工提高自己的安全意识，最终形成恶性循环，导致员工不能严格遵守公司的安全管理制度。人员层次不同，流动性大，安全意识薄弱而产生病毒泛滥、终端滥用资源、非授权访问、恶意终端破坏、信息泄露等安全事件不胜枚举。

所以人员安全部门要定期组织对信息系统所有的工作人员业务及品质两方面进行考核。对指导思想、业务水平、工作表现、遵守安全规程等方面进行考核。对于考核中发现有违反安全法规行为的人员或发现不适于接触信息系统的人员，要及时调离岗位，不应让其再接触系统。

首先，对终身雇员的核实检查应该在应聘时进行，包括令人满意品质的有效证明材料、应聘者个人简历的检查、对应聘者声称的学术或专业资格的确认、身份的查验。此外，还应该制定各岗位的考核制度，定期对不同岗位的人员进行考核，考核包括政治思想、保密观念和业务技术等多个方面。其次，应定期对系统的所有工作人员从政治思想业务水平、工作表现等方面进行考核，对不适于接触信息系统的人员要适时调离。员工从一般岗位转到信息安全重要岗位，组织也应当对其进行信用检查。对于处在有相当权力位置的人员，这种检查应定期进行。那么对工作人员的政治思想水平和工作表现等方面的考核应遵循以下几个方面：

（1）思想政治方面。主要考核是否遵守法律、法规，执行政策、纪律和规章制度，履行职业道德、劳动服务态度等方面。

（2）业务、工作成绩方面。主要依据各自的职责进行考核，相关人员不仅有业务理论水平，还要有实际操作技能。其中对主要职责和实际操作的考核还包括以下几个方面：

① 是否坚持在指定的计算机或终端上操作。

② 程序员、系统管理员和操作员的岗位分离情况。

③ 是否在运行的机器上做与工作无关的操作。

④ 是否越权运行程序，是否查阅无关的操作。

⑤ 是否有操作异常，是否及时上报。

3.4 安全组织机构

3.4.1 安全组织机构的概念

现在计算机信息犯罪者（攻击者）的犯罪（攻击）手段各种各样，技术水平不断提高，防御

者处于被动状态。单靠某一个人或几个人是无法保障信息系统安全的,并且有些攻击或破坏可能来自内部人员,因此必须建立组织机构,完善管理制度,建立有效的工作机制,做到事有人管,职责分工明确。尤为重要的是,要对内部人员进行有组织的业务培训、安全教育、规范行为和制定章程等。

从宏观上讲,《中华人民共和国计算机信息系统安全保护条例》第 13 条规定:“计算机信息系统的使用单位应当建立健全安全管理制度,负责本单位计算机信息系统的安全保护工作”。

从微观上讲,《计算机信息系统安全保护条例》第 4 条明确规定:“计算机信息系统的安全保护工作,重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全”。切实保护本单位信息系统的安全,是直接保护本单位权益的需要,更是维护国家利益的需要,还必须从根本上认识到,这是法律所赋予的责任,是有国家强制力作后盾的,是不能不履行的,否则要负法律责任。

安全组织机构就是为有效实施信息安全管理,保障和实施系统的信息安全,在系统内部建立的组织架构。

高层管理者(如本单位信息化领导小组)负责重大决策,提供资源并对工作方向、职责分配给出清晰的说明。

不仅仅由信息化技术部门参与,与信息安全相关的部门(如行政、人事、安保、采购、外联)都应参与到组织体系中,各司其职,协调配合。

3.4.2 安全组织机构的目标

安全组织机构的控制目标,简单来说,就是在组织机构中管理信息安全。即应当建立适当管理架构,在组织机构内部启动和控制信息安全的实施。

管理层领导应当建立适当的信息安全管理委员会,以便确认信息安全策略、指派安全角色,并在组织机构中协调安全措施的实施。如果需要的话,应当建立一个信息安全专家建议的资料来源并使其在组织机构内部是可以利用的。应当加强与外部的信息安全专家的联系,以跟上工业发展趋势、监控安全标准和测评方法,并在处理意外安全事故时提供适当的联络点。应当鼓励发展那些综合了各学科知识的信息安全解决方案。例如,此综合解决方案可能涉及经理、用户、管理员、应用程序设计人员、审计人员和安全人员的协调和合作,以及在一些领域的特定技术,如保险和风险管理。

为了确保上述目标的实现,可以从以下几方面采取措施。

(1) 信息安全管理委员会。信息安全管理委员会确保明确的目标和管理层对启动安全管理可见的支持。管理委员会应通过适当的承诺和提供充足的资源推广安全。

(2) 信息安全协作。在大的组织机构中,应使用一个由各组织机构相关单位的管理者代表组成的跨职能部门的委员会,协作实施信息安全控制措施。

(3) 明确信息安全责任。在机构中,应明确定义保护每种资产和负责特定安全过程的责任。

(4) 对信息处理设施的授权过程。安全组织机构应建立对于新的信息处理设施的管理授权过程。

(5) 专家信息安全建议。应从内部或外部搜集专家的信息安全建议,并在组织机构内

部实施协作。

（6）组织机构间的合作。应当与执法机关、主管机关、信息服务提供者及通信业者维持适当的接触。

（7）独立的信息安全审查。应对信息安全方针的实施进行独立的审查。

3.4.3　安全组织机构的实例

安全组织作为一个综合性的组织，其运行应独立于信息系统的运行。而要成功建立一个安全组织机构，也是需要遵循一定规则和达到一定要求的。首先，要明确建立安全组织机构的要求；其次，清楚组织机构的基本任务；最后，要确立组织中需要严格遵守的规章制度。只有这样才能建立起真正意义上的安全组织机构。

1. 建立安全组织机构的基本要求

（1）安全组织机构应当由单位安全负责人领导，绝对不能隶属于计算机运行或计算机应用部门。

（2）该安全组织是本单位的常设工作职能机构，其具体工作应当由专门的安全负责人负责。

（3）安全组织的成员类型主要有硬件、软件、系统分析、审计、人事、保卫、通信、本单位应用业务，以及其他所需要的业务技术专家等人员。

（4）该组织一般有着双重的组织联系，即接受当地公安机关计算机安全监察部门的管理、指导，以及与本业务系统上下级安全管理工作相联系。

2. 明确安全组织机构的基本任务

基本任务是在政府主管部门的管理指导下，由与系统有关的各方面专家，定期或适时进行风险分析，根据本单位的实际情况和需要，确定计算机信息系统的安全等级管理总体目标，提出相应的对策并监督实施，使得本单位计算机信息系统的应用发展建设能够与计算机安全保护工作同步前进。

3. 明确安全组织的基本标准

（1）由主管领导负责的逐级计算机安全防范责任制，各级的职责划分明确，并能有效地开展工作。

（2）明确计算机使用部门或岗位的安全责任制。

（3）有专职或兼职的安全员，行业部门或大型企事业单位应确立计算机委员会、安全组织等逐级的安全管理机制，安全组织人员的构成要合理，并能切实发挥职能作用。

（4）有健全的安全管理规章制度。按照国家有关法律法规的规定，建立、完善各项计算机安全管理规章制度，并落到实处。

（5）在职工群众中普及安全知识，提高信息安全意识，对重点岗位的职工进行专门的培训和考核，持证上岗。

（6）定期进行计算机信息系统风险分析，并对信息安全实行等级保护制度，本着保障安全、有利于生产（工作、发展）和注意节约的原则，制定安全政策。

（7）在实体安全、信息安全、运行安全和网络安全等方面采取必要的安全措施。

（8）对本部门计算机信息系统的安全保护工作有档案记录和应急计划。

（9）严格执行计算机信息系统案件上报制度，对信息系统安全隐患能及时发现并及时

采取整改措施。

（10）对信息系统安全保护工作定期总结评比，奖惩严明。

安全管理至少有9个主要环节，即领导重视、组织落实、采取等级保护体制、责任分解明确并落实到人、具体措施到位、各类安全管理制度健全、建立安全技术保障、周密细致的信息安全工作、严格周详的审计应急计划。例如，信息安全领导小组是各级系统网络与信息安全工作的最高领导决策机构，它不隶属于任何部门，直接对本单位最高领导负责，信息安全领导小组是一个常设机构（负责本单位信息安全工作的宏观管理）。各级信息安全领导小组的组长一般由各级系统的高层领导挂帅，并结合与信息安全相关各职能部门的主要负责人参加。

3.5 资产管理

3.5.1 资产管理的概念

资产通常包括业务数据、合同协议、科研材料、操作手册、系统配置、审计记录、制度流程等；应用软件、系统软件、开发工具；计算机设备、通信设备、存储介质；安全防护设备；通信服务、供暖、照明、能源；人员；无形资产，如品牌、声誉和形象。

资产管理可从以下几个方面进行。

（1）组织可以根据业务运作流程和信息系统拓扑结构来识别信息资产。

（2）按照信息资产所属系统或所在部门列出资产清单。

（3）所有的信息资产都应该具有指定的属主，并且可以被追溯责任。

（4）信息应该被分类，以标明其需求、优先级和保护程度。

根据组织采用的分类方案，为信息标注和处理定义一套合适的程序。

3.5.2 资产管理的目标

案例3.1 某单位欲安装一台网络防火墙，却发现没有人可以说清楚当前的真实网络情况，也没有人能说清楚系统中有哪些服务器，这些服务器运行了哪些应用系统。

案例3.2 某单位信息安全评估，发现大部分服务器安全状况良好，只有一台服务器存在严重安全漏洞。研究整改措施时，发现平时没有人对该服务器的安全负责。

从以上案例能看出，公司在资产管理方面资产责任不明确，信息分类十分模糊。这就要求在实现资产管理时必须要达到如下两个目标。

（1）资产责任。实现并保持组织资产的适当保护。列出资产清单，明确保护对象；明确资产受保护的程度；明确谁对资产的安全负责。

（2）信息分类。确保对信息资产的保护达到恰当的水平。根据信息的价值、法律要求和对组织的敏感程度进行分类；信息类别标识，如表明文件的密级、存储介质的种类、内网专用U盘；规定重要敏感信息的安全处理、存储、传输、删除和销毁的程序。

3.5.3 资产管理的实例

关注点、重点不同直接影响信息的分类。军事机构更加关注机密信息的保护，私有企业

通常更加关注数据的完整性和可用性。现举例私有企业和军事机构信息分类比如表 3.2 所示。

表 3.2 私有企业和军事机构信息分类比

状态	定　　义	实　　例	使用分级的组织
公共	即使泄露不会给公司或个人造成不利影响	有多少人完成某个项目	商业公司
私有	可能给公司或个人带来不利影响	人事资源信息	商业公司
绝密	如果泄露会给国家安全带来毁灭性破坏	新型战时武器设计图	军事机构
秘密	给国家安全造成重大威胁	核弹部署	军事机构
不保密	非保密信息	计算机手册	军事机构

3.6 物理与环境安全

3.6.1 物理与环境安全的概念

新世纪的第一缕曙光,开启了信息化时代人类文明的新纪元。Internet 正在越来越多地融入社会的各个方面。一方面,网络应用越来越深地渗透到政府、金融、国防等关键领域;另一方面,网络用户成分越来越多样化,出于各种目的的网络入侵和攻击越来越频繁。安全保障能力是新世纪一个国家的综合国力、经济竞争实力和生存能力的重要组成部分。不夸张地说,它将在 21 世纪里完全可以与核武器对一个国家的重要性相提并论。这个问题解决不好将全方位地危及我国的政治、军事、经济和社会生活的各个方面,使国家处于信息战和高度经济风险的威胁之中。

网络面临的安全威胁大体可分为两种：一种是对网络数据的威胁；另一种是对网络设备的威胁。这些威胁可能来源于各种因素：外部和内部人员的恶意攻击,是电子商务、政府上网工程等顺利发展的最大障碍。我国的安全官员认为：没有与网络连接,网络安全威胁便受到限制。国家保密局于 2000 年 1 月 1 日起颁布实施的《计算机信息系统国际联网保密管理规定》第二章保密制度第六条规定："涉及国家秘密的计算机信息系统,不得直接或间接地与国际互联网或其他公共信息网络相连接,必须实行物理隔离。"许多机构要求有效地保障机密数据,防止通过内部环境与外界敌对环境之间的物理联系而遭受网络侵袭。

物理与环境安全就是防止未经授权的进入、访问、破坏及干扰企业运行场所及信息,确保信息处理设施、关键核心设备和数据的安全。

3.6.2 物理与环境安全的目标

案例 3.3 间谍潜入机房,直接用移动硬盘将服务器中的重要数据复制走。

案例 3.4 机房中气温过高,导致计算机无法正常运行,造成业务中断。

案例 3.3 中出现的问题表明,重要数据所处的环境并不属于安全区域,让其他人很容易地就将重要数据复制出去。而案例 3.4 中计算机中的设备由于物理环境不合适,计算机内

部设备无法正常运行。这就对物理与环境安全提出了要求。

（1）设备要处于安全区域，防止非授权访问、破坏和干扰业务运行。而要实现这一目标就要具有以下的前提条件及信息。

① 具有物理安全边界。建立安全边界，形成安全区域。

② 物理入口控制。必须弄清来访者的身份，并将其进入与离开安全区域的日期与时间记录下来。所有人员必须佩戴识别证。

③ 区域安全。关键设备应放在公众无法进入的地方；并写上“机房重地，请勿进入”的字样；安全区内，各种打印机、复印机设备齐全。

（2）保证设备的安全，预防资产的丢失、损坏或被盗，以及对组织业务活动的干扰。可以从以下几点保证设备的安全。

① 设备安置和保护。保证电力的正常供应，这关系到企业的营运是否正常。要防止电源故障与供电不正常的现象。

② 设备运行的良好环境。建设一个好机房，应当参照有关国家标准，如《电子计算机机房设计规范》(GB 50174—93)。机房的选址和设备的放置要考虑火灾、地震、洪水风暴等可能的自然威胁，以及爆炸、蓄意破坏、盗窃、恐怖袭击、暴动等可能的人为威胁。机房、办公场所和通信线路铺设需要考虑通信中断、电力中断等支撑性基础设施失效的问题。

③ 布缆安全。电源线路应该使用地下暗线；电力线路应与通信线路隔离，以避免相互干扰。

④ 设备维护。按照供应商推荐的服务间隔与规范，对设备进行维护。

⑤ 组织场所外的设备安全。笔记本电脑的取走使用，必须经过授权。

⑥ 设备的安全处置和再利用。对于储存敏感设备的储存设备，必须销毁或是重写数据资料，不可以只使用简单的删除功能。

3.6.3 物理与环境安全的实例

1. 围墙和门

提供物理安全的一种最古老和最可靠的方法是，以围墙和门的形式提供控制，阻止对设施的非授权访问。太高而不容易被爬上去的围墙，可以防止很大一部分的非法入侵，也使保安人员容易发现非法进入的人员，造价不高且效果明显。计算机机房的所有房门都应该足够结实，能防止非法的进入。计算机机房宜设单独出入口，当与其他部门共用出入口时，应避免人流、物流的交叉。为工作而设置的房门应尽可能少，以便容易控制进入机房的人员。为了加强门的保护能力，可以将门连接到外围警报系统，当门被打破时，可以发出警告信号，这可以通过电子设备门实现。

2. 警卫

重要的安全区应该设置警卫，警卫具有应用推理能力。警卫应该仔细检查进入者的证件和使用手册，检查参观人员的有效许可证明，防止未经许可的人员进入安全区。要对移出安全区域的设备和媒体进行检查，接收注册的信件，并做好详细的记录，以备核查。特别需要说明的是，为选择合适的警卫，应该查看他过去的简历以及他是否接受过有关培训，这是很重要的。例如，如果一个警卫负责检查磁带、磁盘和其他计算机介质，他就必须认识它们，并懂得它们是什么。

3. 警犬

如果机构要保护价值很高的资源，警犬就是物理安全的一个很有价值的部分，但警犬必须正确地纳入计划中，进行适当的管理。警犬很有用，因为其敏锐的嗅觉和听力可以检测到警卫不能检测到的入侵。警犬可置于危险的环境中，从而使人不必冒生命危险。

4. ID 卡和证章

将物理安全与信息访问控制紧密联系的一个领域是使用身份证(ID)和名字证章。ID卡的磨损一般是看不出的，而名字证章是可见的。这些设备有许多用途，首先，它们可用作生物测定学的简单形式，通过面容识别一个人，验证它对设备的访问权限。ID 卡可以用某种可见的方式编码，作为访问某些大楼或区域的进门卡。其次，ID 卡的磁条或无线芯片可以由自动控制设备识别，因此，机构就可以给能访问设施内受限区域的人授权。然而，ID 卡和名字证章不是很牢靠，ID 卡很容易被复制、窃取和修改。由于有这个内在的漏洞，这些设备不应是受限区域的唯一访问控制措施。

这类物理访问控制技术的另一内在漏洞是人为因素，这称为“跟进”：授权人拿出钥匙，打开门后，其他已授权或未授权的人也随之进入。让员工警惕“跟进”是解决此问题的一种方式。也有基于技术的方式来避免跟进，如捕人陷阱和十字转门。这些额外的控制措施通常很昂贵，因为它们需要一定的楼层空间和建造费用，对需要使用它们的人来说也不方便。因此，反跟进控制只能在特别关注员工授权进入时使用。

5. 钥匙和锁

除了极其重要的安全区，所有机房的出入完全由门卫控制，虽然安全性高，但太麻烦，也不太实际。一般情况下，还是以有授权的工作人员使用钥匙最为普遍，但是钥匙可能会落入别人手里，这就需要对工作人员加强教育，仔细保护好自己的钥匙。如果钥匙丢失，要及时报告并换锁。一些工作区，应该由专人管理钥匙，并制定严格的交接制度以保证安全。所有的人员在离职后，都应该交出所有相关钥匙并考虑换锁。还有一条规则是要保证钥匙有备份，以便管理人员不在时其他人员在被授权的情况下能打开锁。

锁是大量使用的保护装置，如果钥匙被非授权者拿到或复制，那么对非授权者来说，就没有了任何限制，而且有技能的入侵者可能不用钥匙就能打开锁。对于机房来说，可以考虑采用以下几种锁。

(1) 传统的钥匙和锁。耗费是最小的，几乎每扇门都可以装备，然而钥匙很容易被复制，钥匙持有者可以随时进入，对于东西的出入没有任何控制。

(2) 精选的抵抗锁。与传统锁相比，费用大概是 2～3 倍，钥匙很难被复制，其他特征跟传统锁一致。

(3) 电子组合锁。这种锁使用电子按动按钮进入，有些在一定情况下允许输入特别代码来打开门，但同时会引发远程告警。

(4) 机械按钮组合锁。按下正确的组合可以撤销门闩，打开门。相比电子锁而言，其可靠性差，但费用低。

6. 捕人陷阱

在高安全领域，通常增强锁的形式是捕人陷阱。捕人陷阱是一个入口点和出口点不同的小围栏。每个进入设施、区域或房间的人都先进入捕人陷阱，通过某种形式的电子或生物测定学锁和钥匙请求访问，如果通过了检查，就退出捕人陷阱，进入设施。如果一个人被拒

绝进入,则捕人陷阱就不允许他退出,直到安全官员打开此围栏的自动锁为止。

7. 电子监视

要记录特定区域内警卫和警犬可能遗漏的事件,或记录其他物理控制无效的区域内的事件,可以使用监视设备。许多人都见过很多零售店天花板上安装的银球灯装置,这些摄像机从各个角落对来人进行观察,这就是视频监视。这些摄像机的另一端是录像机(VCR)以及捕获视频信号的相关设备。电子监视包括闭路电视系统(CCT)、一些 CCT 搜集视频信号、其他一些 CCT 接收诸多摄像机的输入,依次对每个区域进行采样处理。

这些视频监视系统存在一些弊端:大部分是被动的,不能阻止访问或被禁止的活动;另一个缺点是其他人也处于实时监视状态下。目前还没有开发出能够可靠地评估这些数据的智能系统,也就是说,为了判断是否发生了未授权的活动,安全人员必须实时查看信息,或查看录下的监视信息。因此,CCT 常常用于收集已入侵区域的数据,它是一个证据收集设备,而不是检测设备。然而,在安全性级别要求很高的区域(如银行、娱乐场所和购物中心)里,安全人员需要不断地监视 CCT 系统,查找非法的活动或可疑的活动。

8. 警报和警报系统

与监视紧密相关的是警报系统,它在预判断的事件或活动发生时通知相关人员。警报可用于检测物理入侵或其他未预料的事件,这可能是火灾、闯入或入侵行为、环境扰动(如洪水)、或服务中断(如断电)。警报系统的一个例子是居民或商务环境中常见的夜贼警报,夜贼警报检测对未授权区域的入侵行为,并通知本地或远程安全机构。为了检测入侵,这些系统依赖于不同类型的传感器,如运动传感器、热量传感器、玻璃损坏传感器、重量传感器和接触传感器。运动传感器检测某一限制空间里的运动,可以主动检测或被动检测。某些运动传感器会发出能量光束,通常是红外线或激光、超声波或声波以及电磁辐射的某种形式。如果发射到受监测区域的能量光束被打断,就发出警报。其他类型的运动传感器是被动的,它们不断地测量受监测区域的能量(红外线或超声波),检测这些能量的快速变化。这些能量的被动测量可以阻止或伪装,因此很容易造假。热量传感器的工作方式是:检测房间里温度变化的速率。它可以用于下面的情形:体温为 98.6 华氏度的人进入一个 65 华氏度的房间,因为人的出现会改变房间的温度。热量传感器也可用于火灾检测。接触传感器和重量传感器在两个面接触时开始工作。例如,脚踩在下面有压力传感器的地毯上,或打开窗户时触动了针头弹簧传感器。振动传感器也属于此范畴,但它们检测的是传感器的运动,而不是环境的变化。

9. 计算机机房和配电室

计算机机房和配电布线室是需要特别注意确保信息的机密性、完整性和可用性的设施。如果攻击者获得了计算设备的物理访问,则很容易击溃逻辑访问控制。能进出机构办公室的人中,保管人员常常是最不引人注目的员工和非员工,然而,他们拥有最大限度的无人监管访问权利。经常出现管理人员把整个大楼的钥匙交给他们以后忘记收回的情况。保管人员要从每个办公室中收集纸张、擦桌子、搬动各个区域的大抽屉。因此对于这类人来说,收集重要的信息和计算机媒体、复制专用的机密信息并不困难。这不是说机构应总是怀疑保管人员可能是间谍,而是指出,保管人员有这么大的权限,很容易被竞争对手利用,来获得未授权的信息。他们不但应由机构的一般管理层来管理,还应由 IT 管理层来管理。

3.7 访问控制

3.7.1 访问控制的概念

访问控制系统及其方法论所要处理的课题和问题,涉及准予或限制用户对资源进行访问时的监控、标识和授权。通常,访问控制是指所有对访问进行授权或限制的硬件、软件、组织机构管理策略或程序,他们监控和记录访问的企图,标识用户的访问企图,并且确定访问是否经过了授权。

控制对资源的访问是安全性的中心话题。访问控制所涉及的内容要比简单地控制哪些用户可以访问哪些文件或服务多得多。访问控制是对主体和客体如何结合的管理,从客体到主体的信息传输叫做访问。主体(Subjects)是活动的实体,它通过访问操作,寻找有关被动实体的信息,或者从被动实体中寻找数据。这个被动实体也可称为客体(Objects)。主体可以是用户、程序、进程、文件、计算机和数据库等。客体可以是文件、数据库、计算机、程序、进程、打印机和存储介质等。主体是接收有关客体的信息或来自客体的数据实体。主体还是改变客体信息的实体,或改变存储在客体中数据的实体。客体始终是提供、控制信息和数据的实体。主体和客体之间进行通信,执行一项任务时,两个实体的角色可以交换,如程序和数据库、处理进程和文件。

访问控制对于保护客体(其信息和数据)的保密性、完整性和可用性是很有必要的。术语访问控制可以用来描述广泛的控制,包括从强制用户提供有效的用户名和密码进行登录操作,到防止用户获得对资源超出其访问权限的操作。

3.7.2 访问控制的目标

之所以要实施访问控制,是为了实现下面这几个目标。

(1) 访问控制的业务需求——控制对信息的访问。

(2) 用户访问管理——确保授权用户的访问,并预防信息系统的非授权访问。

(3) 用户责任——预防未授权用户的访问,信息和信息处理设施的破坏或被盗。

(4) 网络访问控制——防止对网络服务未经授权的访问。

(5) 操作系统访问控制——防止对操作系统的未授权访问。

(6) 应用访问控制——防止对应用系统中信息的未授权访问。

(7) 移动计算和远程工作——确保在使用移动计算和远程工作设施时信息的安全。

然而访问控制有许多种,而每种方式都起到不同的作用。所有的访问控制都是为了实现以上目标而工作,但是每种访问控制又有其不同的侧重点。

1. 预防性访问控制

进行预防性访问控制是为了阻止不必要的或未授权的操作出现,如预防性访问控制包括防护、安全策略、安全感知训练和反病毒软件。

2. 纠正性访问控制

进行纠正性访问控制是为了在不必要的或未授权的操作发生后将系统恢复到正常的状态,如纠正性访问控制包括报警、圈套和安全性策略。

3. 行政性访问控制

行政性访问控制是依照机构的安全性策略定义的策略和执行过程，实现并加强全局的访问控制，如行政性访问控制包括策略、执行过程、雇佣准则、背景调查、数据分类、安全培训、空缺记录、回顾、工作监督、人员管理和测试。

4. 逻辑/技术性访问控制

逻辑性访问控制和技术性访问控制作为硬件或软件机制，可以用来管理对资源和系统的访问，并且提供对这些资源和系统的保护，如逻辑性访问控制和技术性访问控制包括加密、智能卡、密码、生物测定学、受限接口、访问控制列表、协议、防火墙、路由器、入侵检测系统和切割层。

5. 物理性访问控制

物理性访问控制作为物理屏障，可以用来保护对系统的直接访问，如物理性访问控制包括防护装置、移动探测器、闭锁的门、密封窗、灯光、线缆保护、笔记本电脑锁、刷卡、狗、摄像机、圈套和警报器。

访问控制控制着主体对客体的访问。这个过程的首要步骤是对客体进行标识。实际上，在对客体的实际访问之前还有几个步骤需要执行，即标识、验证、授权和责任衡量。

标识是一个主体表示其身份并进行责任衡量的过程。提供用户名、登录 ID、个人身份号码或智能卡的用户向我们描述了标识的过程。一旦主体完成了标识，那么这个身份标识就要对主体所做的进一步操作负责。信息技术系统通过身份标识来跟踪实际的操作，而不是通过主体自身进行跟踪。一台计算机并不认识我们，但是它却知道操作者的用户账号与其他人的用户账号是不同的。

验证是指对所宣称的身份标识的有效性进行校验和测试的过程。验证需要主体提供额外的信息，这些信息必须与身份标识所指示的内容完全相符。最常见的验证形式是密码。然而，至少有 3 种其他形式的信息可用于验证。

类型 1 验证因素是指一些大家知道的内容，如密码、个人身份号码（PIN）、母亲的姓和喜欢的颜色等。

类型 2 验证因素是指操作者所具有的内容，如智能卡、凭证设备和内存卡等。它还可以包括操作者的物理位置，被称为“你在哪里”的因素。

类型 3 验证因素是指操作者所具有的一些如指纹、语音波纹、视网膜样本、虹膜样本、面容形状、掌纹和手型等的内容。

一旦将身份标识和验证因素的登录证书提交给系统，那么系统就会将它们与系统中的身份标识数据库进行核对。如果找到了身份标识，并且提供的验证因素也正确，那么主体通过验证。

然而，每当主体通过了验证，其访问还必须经过授权。授权的过程确保了被请求的操作或目标访问可能获得了向经验证的身份标识（将它看作是这里的主体）赋予的权利和特权。大多数情况下，系统会估计一个访问控制矩阵，它会对主体、客体（目标）和预计的操作进行比较。如果指定的操作可以进行，那么主体就已经获得了授权。如果指定的操作没有被准许进行，那么主体就没有获得授权。

需要记住，主体只是经过标识和验证，并不同时意味着已经通过了授权。对于主体来说，登录到网络中（如被标识和验证）却被阻止访问文件或从打印机打印是可能的（如没有经

过授权来执行这项操作)。大多数网络用户只是被授权在指定的一组资源上执行一些有限的操作。身份标识和验证是访问控制的重要体现或者不是任何一个方面。对于环境中的每个单独的主体和客体,在全部或什么也不是之间,授权有着很大的区别。用户可能能够读取文件,却不能删除它。用户可能能够打印文档,但是不能修改打印队列。用户可能能够登录到系统中,但是无法访问任何资源。

理解身份标识、验证和授权之间的区别是很重要的。虽然它们很相似,并且是所有安全机制的本质内容,但它们是不同的,并且必须搞清楚,不能混淆。这些功能在本章稍后的内容中将进行非常详细的分析。

一个机构的安全策略只能在支持责任衡量的情况下,才可以正确地执行。换句话说,只有在主体对于它们的操作负有责任时,安全性才可以保证。有效的责任衡量依赖于检验主体的身份和跟踪其操作的能力。因此,责任衡量建立在身份标识、验证、授权、访问控制和审核的概念上。

3.7.3 访问控制的实例

访问控制管理是分配给管理员管理用户账户、访问和责任衡量的一组任务和责任。系统的安全性以有效的访问控制管理为基础。需要记住,访问控制依赖于 4 个原则:身份标识、验证、授权和责任衡量。在涉及访问控制管理时,这些原则转换为 3 个主要的职责:用户账户管理;操作跟踪;访问权利和许可权的管理。

1. 用户账户管理

用户账户管理涉及建立、维护和关闭用户账户。虽然这些操作可能看起来很普通,但是对于系统访问控制效力来说却是必要的。没有正确定义和维护的用户账户,系统就不能建立标识、实施验证、证实授权或跟踪责任。

新用户账户的建立是一个简单的系统处理过程,但是它必须受到组织机构安全性策略的保护或保障。用户账户不应该凭管理员的一时兴起或任何人的请求而建立;相反,应该遵循人事部门的雇佣或职务提升手续执行严格的操作。

人事部门应该对新员工的用户账户做出证实的要求。要求应该包括分配给新员工用户账户的分类或安全性级别。新员工的部门经理和公司安全管理员应该检验安全分配。只有要求得到了验证,才能随后建立新的用户账户。不遵循已建立的安全性策略和手续建立用户账户,会带来漏洞和疏忽,被恶意主体所利用。增加或减少现有用户账户安全性级别也应遵循类似的过程。

作为人员雇佣的手续,新员工应该接受公司安全性策略手续的培训。在完成雇佣前,员工应该签署一份协议,承诺支持公司的安全标准。许多组织机构已经选择构思一份文档,规定违反安全性策略就会被解雇,以及依照我国法律进行起诉。当将用户的账户 ID 和临时密码交给新员工时,应当执行密码策略(Password Policy)的检查和可接受的使用约束。

新用户账户的最初建立常常被称为注册。注册过程生成新的身份,并建立起系统进行验证所需要的要素。正确并完整地完成注册过程是很关键的。通过组织机构采用的任何必要且充分的手段对注册个体的身份进行证实也是很关键的。在向安全系统注册这些人时,带照片的身份证、出生证、背景调查、信用调查、安全性级别证实,甚至职业证明都是证实一个人身份的有效形式。

用户账户的整个生命周期内，持续的维护是必不可少的。那些有着相当稳定的组织结构和较少人员变动或升迁的组织，比起那些有着灵活的或动态的组织结构并且具有较高的人员变动和升迁的组织，将具有较少的账户管理工作。大多数账户维护工作围绕着账户的权限和特权的更改而进行。应当建立起类似于新账户建立时的那些过程，它们管理着在整个用户账户的生命周期内对访问的更改。未授权账户访问能力的增加或减少会产生严重的安全影响。

当一个员工不再为公司工作时，其用户账户应该被关闭、删除或废除。无论何时，只要可能，这项工作就应该自动完成，并且应当与人事部门相配合。在大多数情况下，当薪水停止支付的时候，这名员工就应不再具有登录的能力。临时或短期的员工应当在他们的用户账户中拟订特定的截止日期。这样得以维护账户生成时建立的控制级别，并且不会出现管理疏漏。

2. 账户、日志和定期监控

操作审计、账户跟踪和系统监控也是访问控制管理中的重要内容。没有这些内容，把握主体责任将是不可能的。在身份建立、验证和授权的过程中，跟踪主体的操作(包括他们访问了客体多少次)提供了直接且明确的责任。

3. 访问权限和许可权管理

为客体分配访问权限是实施组织机构安全性策略的重要部分。不是所有的主体都应当被赋予对所有客体的访问权限，也不是所有的主体都应具有相同的功能。一些特定的主体只应当访问一些客体，某些功能只应当由一些特定的主体访问。

最少特权的原则来自于当主体被赋予对客体进行访问的权限时所形成的复杂结构。这个原则规定主体只应当被授权访问那些完成其工作所需要的客体。换而言之，应当阻止主体访问那些工作内容不需要的客体。

决定哪些主体对哪些客体具有访问权限，这是组织机构安全性策略、人员所在的组织层次和访问控制模型实施的一项功能。因此，建立或定义访问权限的标准可以建立在身份、角色、规则、分类、位置、事件、接口和需要知道的等基础上。

讨论对客体的访问要用到 3 个主体标记：用户、所有者和管理人。用户就是任意的主体，他可以访问系统中的客体，执行一些操作或完成工作任务。所有者是对分类和标记客体、保护和存储数据负有最终责任的人。如果所有者在建立、执行安全性策略保护和维护敏感数据时没有做到很充分，那么可能要对疏漏承担责任。日常要对客体进行适当的存储和保护工作，被分配或委派了这种工作的人称为管理员。

用户就是系统中的任意最终用户。所有者常常就是 CEO、董事长或部门领导。管理人员常常就是 IT 人员或系统安全管理员。

任务和责任分离是通用的准则，它防止任意单一的主体回避或禁用安全机制。当核心管理或高级授权责任被分为几个主体时，没有一个主体具有足够的访问权限来执行有恶意的操作或绕过强迫执行的安全控制。任务的分离建立了一个检测和平衡系统，在这个系统中，多个主体可以相互校验操作，并且必须一起完成必要的工作任务。任务分离使得恶意的、欺诈的或其他未授权的操作变得更加困难，并且拓宽了检测和报告的范围。对于个人来说，如果他们认为可以侥幸成功，那么执行未授权的操作是简单的。一旦涉及两个或更多的人，那么未授权操作的承诺需要每个人同意保密才行。这通常会作为一种有效的威慑，而不

是贿赂一组人的手段。

3.8 符合性管理

3.8.1 符合性管理的概念

案例 3.5 目前,Internet 上至少有 3 万多个公开的黑客网站,这些网站除了黑客知识与技能的培训外,还提供了大量的黑客工具,一个稍具计算机知识的中学生经过黑客网站的培训,利用下载的黑客工具就可以发起有一定威胁性的攻击。最近有人甚至在网上以几百元的价格兜售定制的病毒。

但同样的情况如果发生在现实生活中,结果就不一样了。比如有人想办一个小偷培训学校,可能还没开张就被取缔了;很少有人敢故意培养并散布传染病病毒,否则必将受到法律的严惩。

解决信息安全问题不能仅依靠安全技术,制定并执行一系列完善的法律、法规才是保护信息安全的重要手段。

符合性管理就是要避免违反法律、法规、规章、合同的要求,以及本单位安全策略和制度标准的规定。

3.8.2 符合性管理的目标

(1) 具有与法律法规要求的符合性。避免违反法律、法规、规章、合同要求和其他的安全要求。

(2) 符合安全方针、标准,技术符合性。确保系统符合组织安全方针和标准。

(3) 信息系统审核的考虑因素。最大化信息系统审核的有效性,最小化来自对信息系统审核的影响。

3.8.3 符合性管理的实例

首先,要明确适用于本单位的有关国家法律法规、合同条款和正在执行的本单位策略和制度。例如,各国的银行业一般都有针对银行数据保护的立法,如果由于数据备份恢复程序不完整而造成服务中断,将面临监管部门的严厉处罚。再如,许多国家已立法对互联网上的服务提供商在保护客户信息的保密性及维护服务的可用性方面进行了约束。其次,要使有关人员知悉以上要求,以及为满足这些要求应当遵守的行动规范。最后,通过审核和奖惩制度保证符合性的落实。

3.9 本 章 小 结

本章系统地讲解了基本信息安全管理的概念。信息安全管理概述主要描述了何为信息安全管理,如何进行信息安全管理和进行管理的具体内容。后面的章节则将信息安全管理中需要理解和掌握的概念进行了重点描述和举例。

本章按照信息、信息安全、信息安全管理的顺序层层解析基本信息安全管理。读者需要

先理解安全策略，掌握其概念和内容；然后学习管理方面的知识。管理又分为人员安全管理和资产管理：人员管理中需要掌握人员管理的概念，清楚各阶段的人员管理要采取的不同措施以及措施的具体内容；资产管理中要掌握资产的概念和分类，也要清楚不同的资产有其不同的分类方法，如军事机构信息的分类。接下来主要介绍的是如何进行安全管理，分为从内部进行管理和通过控制外部环境进行管理。内部管理可以建立安全组织机构，这就要求读者掌握安全组织机构的建立过程，建议读者结合实例理解概念更为容易。外部管理即为保证物理与环境安全，采取恰当的访问控制方法。而要保证物理与环境安全就要了解物理与环境安全的概念和种类，对实例进行了解，并在实际中加以应用。对于访问控制则要掌握其分类和每一类所能达到的目标。最后，无论对信息做出怎样的管理，都要遵循符合性管理的原则，熟知符合性管理的要求，对信息的安全做出正确、有效的管理。

第 4 章　重要信息安全管理措施

导入语：本章系统地介绍了重要信息安全管理措施方面的内容，包括系统获取开发和维护、信息安全事件管理与应急响应和业务连续性管理与灾难恢复 3 个部分。本章主要知识结构如图 4.1 所示。

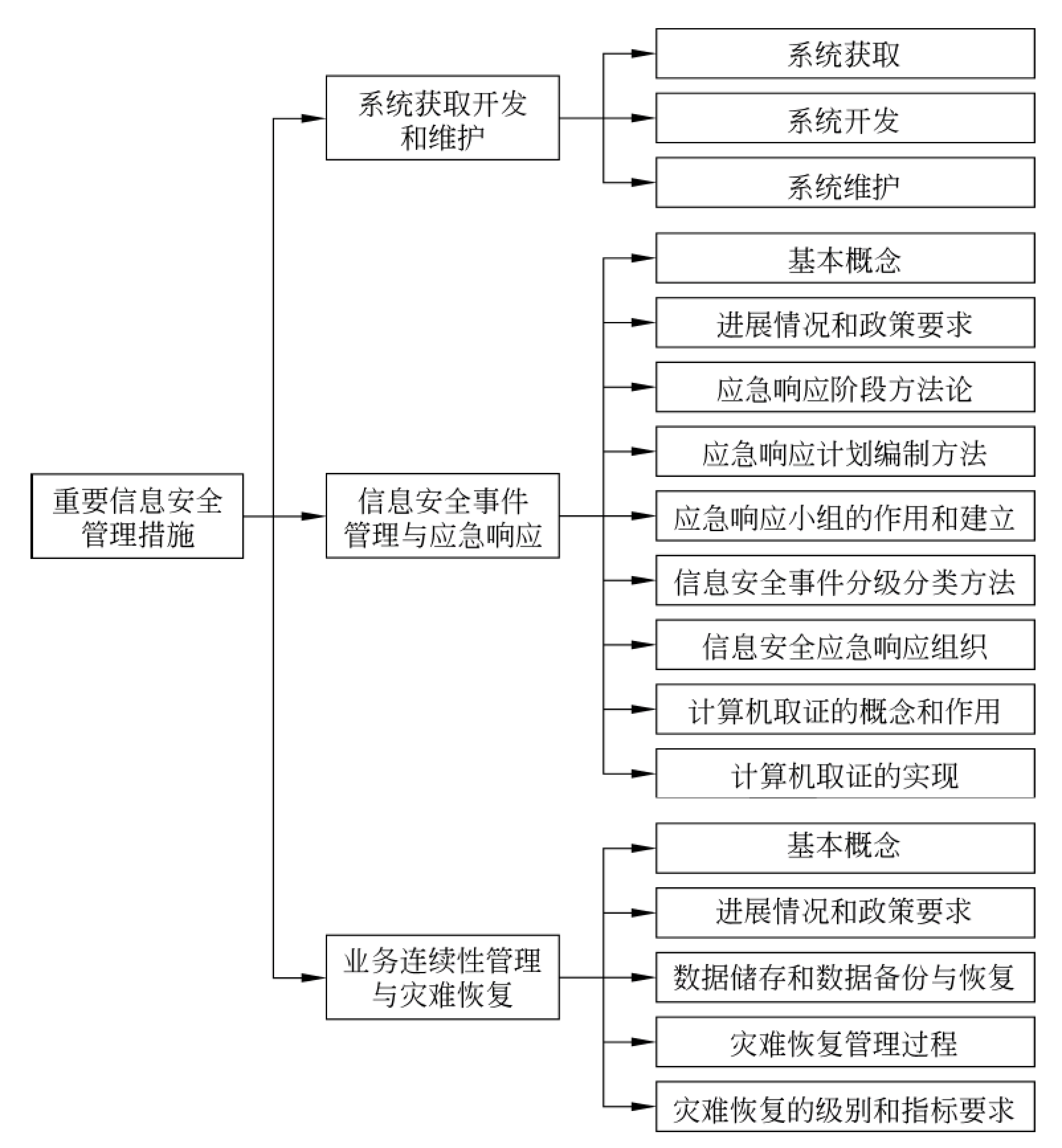


图 4.1　本章主要知识结构图

系统获取开发和维护部分，介绍了系统获取、系统开发和系统维护。

信息安全事件管理与应急响应部分，详细介绍了信息安全事件管理与应急响应的基本概念、我国信息安全事件管理与应急响应工作的进展情况和政策要求、信息安全应急响应阶段方法论、信息安全应急响应计划编制方法、应急响应小组的作用和建立方法、我国信息安全事件分级分类方法及国际和我国信息安全应急响应组织。也介绍了计算机取证的知识，包括计算机取证的概念和作用以及计算机取证的原则、基本步骤、常用方法和工具。

业务连续性管理与灾难恢复部分，详细介绍了业务连续性管理与灾难恢复，主要包括业务连续性管理与灾难恢复的基本概念、我国灾难恢复工作的进展情况和政策要求、数据储存和数据备份与恢复的基本技术、灾难恢复管理过程，同时介绍了国家有关标准对灾难恢复系

统级别和各级别的指标要求。

考核目标：理解安全要求是信息系统需求的重要组成部分，理解信息技术产品采购的安全原则，即符合标准法规、风险与经济性的平衡、安全性测试等，理解信息系统开发和实施的安全原则，规范的开发方法，严格的源代码测试，对安装包、测试数据和程序源代码的保护，理解系统运行阶段安全管理的基本原则，包括漏洞和补丁管理、系统更新、废弃等。

理解信息安全事件管理和应急响应的基本概念，了解我国信息安全事件应急响应工作的进展情况和政策要求，掌握信息安全应急响应阶段方法论，掌握信息安全应急响应计划编制方法，掌握应急响应小组的作用和建立方法，理解我国信息安全事件分级分类方法，了解国际和我国信息安全应急响应组织，了解计算机取证的概念和作用，了解计算机取证的原则、基本步骤、常用方法和工具。

理解业务连续性管理与灾难恢复的基本概念，了解我国灾难恢复工作的进展情况和政策要求，了解数据储存和数据备份与恢复的基本技术，掌握灾难恢复管理过程（需求分析、灾难恢复策略制定、灾难恢复策略实现、灾难恢复预案制定和管理），掌握国家有关标准对灾难恢复系统级别和各级别的指标要求。

4.1　系统获取开发和维护

4.1.1　系统获取

1. 安全信息系统获取的基本原则和方法

安全信息系统获取的基本原则主要为以下 3 个方面：

（1）符合国家、地区及行业的法律法规。

（2）量力而行，达到经济性与安全性间的平衡。

（3）符合组织的安全策略与业务目标。

安全信息系统的获取策略可分为：外部采购；自主开发或者自主开发与外包相结合；采取何种获取策略在项目立项与可行性分析过程中得出结论。

2. 安全信息系统购买

安全信息系统购买流程主要分为 7 个步骤：需求分析、市场招标、评标、选择供应商、签订合同、系统实施、系统运维，如图 4.2 所示。

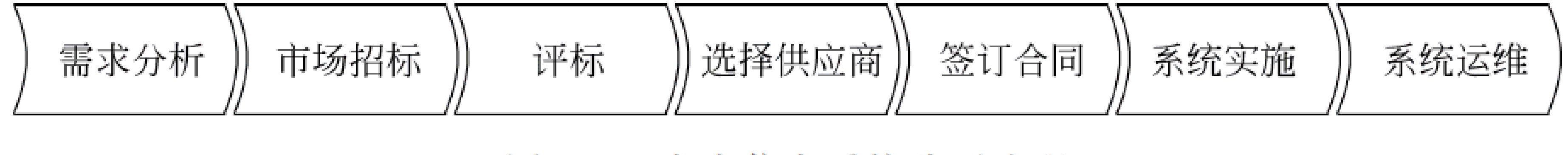


图 4.2　安全信息系统购买流程

（1）需求分析。根据业务需求、法律法规、客户需求，导出各项系统需求。其中包括安全需求；建立初级威胁模型，进行初步风险分析；建立安全目标并进行评审；搭建概念原型，验证安全需求。

（2）市场招标。看一看市场上有什么可选的系统；发放请求建议书或者邀标书，书中包含安全需求相关的描述章节。

（3）评标。评价供应商反馈信息，对可用系统进行横向比较。其中包括供应商安全服

务资质，财务状况，产品安全等级，产品性能，服务容量，服务承诺，售后服务能力等；对信息系统的应用案例进行考察，并听取案例用户以及市场反馈；试用信息系统，比对安全目标，进行安全评测。

(4) 选择中标供应商，并签订合同源代码委托(Source Code Escrow)。签订的合同应该包括以下内容：安全紧急响应条款；售后服务协议；安全培训；业务连续性与灾备条款。在评价供应商时需要考虑一些关键的性能指标：

① 周转时间(Turnaround time)。发生故障时帮助台或厂商从登录系统到解决问题所需的时间。

② 响应时间(Response time)。系统响应一个特定的用户查询所需的时间。

③ 系统反应时间(System Reaction time)。登录到系统或连接到网络所需要的时间。

④ 吞吐量(Throughput)。单位时间内系统的有效工作量。

⑤ 负载(Workload)。执行必要工作的能力，或系统在给定时间区间内能够完成的工作量。

⑥ 兼容性(Compatibility)。供应商提供的新系统对现有应用的运行支持能力。

⑦ 容量(Capacity)。新系统处理并发网络应用请求的数目，以及系统能够为每个用户处理的数据量。

⑧ 利用率(Utilization)。系统可用时间与故障时间之比。

⑨ 安全等级(Security Grade)。权威机构的测评结果，如 EAL4。

(5) 系统实施。在系统实施过程中，要审查配置，管理临时账户，数据要安全迁移，对用户进行安全培训。

购买系统时要注意安全，主要的安全问题有以下两点：

① 组织保障。组织策略中包含了信息安全要求。项目组中包含关注信息系统安全的成员，如安全主管、IS 审计师、法律顾问等。

② 在购买流程中设定关注信息系统安全的控制过程，并保证控制过程能得到确切执行。如安全需求制定，招标书与请求建议书中关于安全需求的描述章节，供应商系统的安全评测等。

4.1.2 安全信息系统的开发

1. 开发步骤

安全信息系统购买流程主要分为 7 个步骤：需求分析、概要设计、详细设计、系统开发、测试、系统实施、系统运维，如图 4.3 所示。

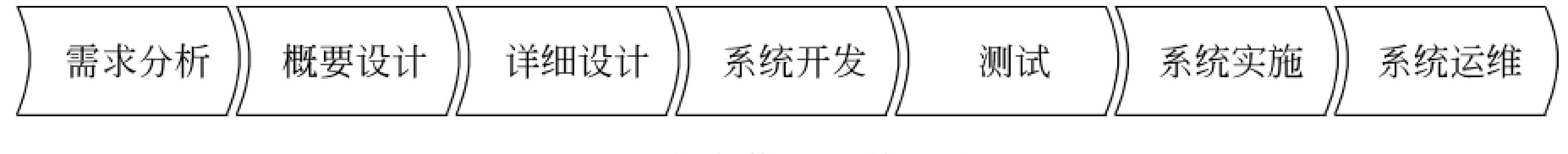


图 4.3 安全信息系统开发流程

在进行需求分析时，应该做到以下几点。

(1) 定义安全需求。其主要包括业务安全需求、法律法规约束以及来自客户的安全要求。

(2) 建立安全需求步骤。

(3) 进行业务安全分析。

(4) 进行业务合规性分析。

(5) 建立威胁模型,进行初步风险分析。

(6) 明确安全风险,建立安全目标列表。

(7) 确定数据通信安全目标、数据存储安全目标、交易完整性目标、身份认证及访问授权目标、审计目标和系统备份与恢复等。

(8) 对安全目标进行评审市场招标。

概要设计主要为详细风险评估与安全控制措施的选择,设计内容包括安全体系架构设计;各功能模块间的安全处理流程;安全协议设计;安全接口设计等。概要设计安全评审选择中标供应商,并签订合同。

详细设计是对安全功能的详细设计,设计内容主要为模块输入安全过滤;模块安全输出;内部处理逻辑安全设计;数据结构安全设计;详细设计安全评审以及评价供应商时的一些关键性能指标。

系统开发是根据安全设计进行开发。为了编写出安全的代码,需要对开发人员实施编码规范培训,进行安全意识教育,为开发人员配备安全编码手册。开发人员要对安全功能实现进行单元测试。同时,开发人员执行代码静态分析,进行代码自查。团队内部进行代码互查,须对源代码进行安全管理。

首先,测试环节对测试用例进行完备性评估;其次,可采用集成测试、系统测试、可接受性测试、渗透测试等测试方法进行测试;最后,进行代码静态分析与代码审查。

最后阶段是系统实施、交付、试运行。在该过程中,要进行配置的审查,对临时账户实施管理,数据要安全迁移,用户需要进行安全培训。

2. 系统开发过程中的安全要素

(1) 开发团队中有比较专业的信息安全人员。

(2) 实施配置管理、基线管理、版本管理、对文档、源代码变更、版本发布进行严格管理。

(3) 配置管理应该贯穿开发周期始终。

(4) 开发,测试环境与生产环境隔离。

(5) 项目管理应该加强对安全控制过程的执行力度。

(6) 使用软件工程方法增强软件质量,减少软件漏洞。

4.1.3 系统维护

为了清除系统运行中发生的故障和错误,软、硬件维护人员要对系统进行必要的修改与完善;为了使系统适应用户环境的变化,满足新提出的需要,也要对原系统做些局部的更新,这些工作称为系统维护。

系统维护的任务是改正软件系统在使用过程中发现的隐含错误,扩充在使用过程中用户提出的新的功能及性能要求,其目的是维护软件系统的“正常运作”。这阶段的文档是软件问题报告和软件修改报告,它记录发现软件错误的情况以及修改软件的过程。

1. 系统维护的内容和类型

系统维护是面向系统中各个构成因素的,按照维护对象不同,系统维护的内容可分为以下几类:

(1) 系统应用程序维护。系统的业务处理过程是通过应用程序的运行而实现的,一旦程序发生问题或业务发生变化,就必然地引起程序的修改和调整,因此系统维护的主要活动是对程序进行维护。

(2) 数据维护。业务处理对数据的需求是不断发生变化的,除了系统中主体业务数据的定期正常更新外,还有许多数据需要进行不定期的更新,或随环境或业务的变化而进行调整以及数据内容的增加、数据结构的调整。此外,数据的备份与恢复等都是数据维护的工作内容。

(3) 代码维护。随着系统应用范围的扩大,应用环境的变化,系统中的各种代码都需要进行一定程度的增加、修改、删除以及设置新的代码。

(4) 硬件设备维护。主要就是指对主机及外设的日常维护和管理,如机器部件的清洗、润滑,设备故障的检修,易损部件的更换等。这些工作都应由专人负责,定期进行,以保证系统正常、有效地工作。

(5) 机构和人员的变动。信息系统是人机系统,人工处理也占有重要地位,人的作用占主导地位。为了使信息系统的流程更加合理,有时涉及机构和人员的变动。这种变化往往也会影响对设备和程序的维护工作。

系统维护的重点是系统应用软件的维护工作,按照软件维护的不同性质划分为下述 4 种类型。

(1) 纠错性维护。由于系统测试不可能揭露系统存在的所有错误,因此在系统投入运行后频繁的实际应用过程中,就有可能暴露出系统内隐藏的错误。诊断和修正系统中遗留的错误,就是纠错性维护。纠错性维护是在系统运行中发生异常或故障时进行的,这种错误往往是遇到了从未用过的输入数据组合或是在与其他部分接口处产生的,因此只是在某些特定的情况下发生。有些系统运行多年以后才暴露出在系统开发中遗留的问题,这是不足为奇的。

(2) 适应性维护。适应性维护是为了使系统适应环境的变化而进行的维护工作。一方面,计算机科学技术迅速发展,硬件的更新周期越来越短,新的操作系统和原来操作系统的新版本不断推出,外部设备和其他系统部件经常有所增加和修改,这就是必然要求信息系统能够适应新的软硬件环境,以提高系统的性能和运行效率;另一方面,信息系统的使用寿命在延长,超过了最初开发这个系统时应用环境的寿命,即应用对象也在不断发生变化,机构的调整,管理体制的改变、数据与信息需求的变更等都将导致系统不能适应新的应用环境。如代码改变、数据结构变化、数据格式以及输入/输出方式的变化、数据存储介质的变化等,都将直接影响系统的正常工作。因此有必要对系统进行调整,使之适应应用对象的变化,满足用户的需求。

(3) 完善性维护。在系统的使用过程中,用户往往要求扩充原有系统的功能,增加一些在软件需求规范书中没有规定的功能与性能特征,以及对处理效率和编写程序的改进。例如,有时可将几个小程序合并成一个单一的运行良好的程序,从而提高处理效率;增加数据输出的图形方式;增加联机在线帮助功能;调整用户界面等。尽管这些要求在原来系统开发的需求规格说明书中并没有,但用户要求在原有系统基础上进一步改善和提高;并且随着用户对系统的使用和熟悉,这种要求可能不断提出。为了满足这些要求而进行的系统维护工作就是完善性维护。

（4）预防性维护。系统维护工作不应总是被动地等待用户提出要求后才进行，应进行主动的预防性维护，即选择那些还有较长使用寿命，目前尚能正常运行，但可能将要发生变化或调整的系统进行维护，目的是通过预防性维护为未来的修改与调整奠定更好的基础。例如，将目前能应用的报表功能改成通用报表生成功能，以应付今后报表内容和格式可能的变化，根据对各种维护工作分布情况的统计结果，一般纠错性维护占21%，适应性维护工作占25%，完善性维护达到50%，而预防性维护以及其他类型的维护仅占4%。可见，系统维护工作中，一半以上的工作是完善性维护。

2. 变更管理

变更管理的目的是对系统变更的合理性、安全性进行控制，使变更通过安全过程进行实施，减少不当变更导致的系统安全问题，保障业务连续运行。

正常的变更管理流程应包括：提交变更申请；审批变更申请；变更开发；对变更开发进行测试评估；接受变更；实施变更。变更注意事项如下。

（1）变更程序需要遵循与全面系统开发项目同样的过程，程序员要进行单元测试、模块测试、集成测试等，保证新功能满足需求，且不影响其他模块的功能。

（2）所有变更信息作为系统的永久文档由用户维护人员保留，所有程序变化的维护记录，应该人工保存和自动化保存。文档的变更应该反映到相关的IT管理活动中去，如灾难恢复、保持文档在最新状态。

（3）有些管理软件提供变更审计轨迹。维护信息包括程序员ID号、变更时间和日期，与变更相关的申请号或者项目号，变更前后的源代码行数。

（4）程序员不能写、修改和删除生产环境数据。根据生产的信息类型，程序员甚至不能进行只读访问（客户信用卡号、安全号、敏感信息等）。

（5）需要用户管理层关注程序员所做的变化或者升级，在进行任何变更之前，程序员必须接到授权。

常见非授权变更情况有以下几种：程序员访问生产系统库；该程序的用户不知道发生的变更；没有正式的变更请求表格和程序；相关管理人员并未在变更表上签字；用户没有在变更表上签字以表明接受变更；修改后的源代码未经适当的编程人员检查；相关管理人员没有在变更表上签字以表明变更可以投入生产环境；程序员为了自身的利益增加一些额外的代码。

3. 紧急变更

程序员、分析员可能通过使用特殊的登录ID来访问生产环境以处理紧急情况。应急ID拥有很大的权限，它的使用必须留有日志，并要仔细审查。紧急修复之后还要采用补救措施，将所有正常的变更控制流程再重新执行一遍。

4. 补丁和漏洞管理

当发布系统后，发现有些程序中有漏洞，能被黑客利用而攻击用户，所以发布相应的措施来对付这些黑客，用一些应用程序来修复这些漏洞，称为“补丁程序”，安装这些补丁程序后，黑客就不会利用这些漏洞来攻击用户。而黑客又会从其他位置来想方设法攻击系统，所以，常有发布一些补丁程序来对付黑客。

目前，从技术和管理两个角度来看，漏洞问题已经有了较为成熟的解决方案。漏洞管理就是这样一套能够有效避免由漏洞攻击导致的安全问题的解决方案，它从漏洞的整个生命

周期着手，在周期的不同阶段采取不同的措施，是一个循环、周期执行的工作流程。一个相对完整的漏洞管理过程包含以下步骤：

（1）对用户网络中的资产进行自动发现并按照资产重要性进行分类。

（2）自动周期性地对网络资产的漏洞进行评估并将结果自动发送和保存。

（3）采用业界权威的分析模型对漏洞评估的结果进行定性和定量的风险分析，并根据资产重要性给出可操作性强的漏洞修复方案。

（4）根据漏洞修复方案，对网络资产中存在的漏洞进行合理的修复或者调整网络的整体安全策略进行规避。

（5）对修复完毕的漏洞进行修复确认。

（6）定期重复上述步骤。

例如，0day 攻击漏洞。0day 泛指所有在官方发布该作品之前或者当天，这主要涵盖了影视、软件、游戏、音乐、资料等方面，由一些特别小组以一定的格式打包发布的数码内容。基本上每个 0day 发布作品中都包含了说明该发布作品的 NFO 文件，该文件主要包括发布小组的信息、发布作品的信息、破解信息等。NFO 文件有专门的软件来查看，其实系统自带的记事本也可以查看。

在计算机领域中，0day 通常是指还没有补丁的漏洞，而 0day 攻击则是指利用这种漏洞进行的攻击。提供该漏洞细节或者利用程序的人通常是该漏洞的发现者。0day 漏洞的利用程序对网络安全具有巨大威胁，因此 0day 不但是黑客的最爱，掌握多少 0day 也成为评价黑客技术水平的一个重要参数。

5. 系统弃置管理

对于弃置的系统要用以下方式进行管理：

（1）残余信息的处理。对残余信息的处理方式有物理摧毁存储介质、存储介质消磁处理、专用设备进行反复数据覆盖或者擦除。

（2）键盘攻击。使用功能软件对弃置系统中的存储介质进行分析。

（3）实验室攻击。使用专有设备对弃置系统中的存储介质进行分析。

4.2 信息安全事件管理与应急响应

4.2.1 信息安全事件管理和应急响应的基本概念

安全事件，是指影响一个系统正常工作的情况。这里的系统包括主机范畴内的问题，也包括网络范畴内的问题，如黑客入侵、信息窃取、拒绝服务攻击、网络流量异常等。

应急响应（Emergency Response），是指组织为了应对突发/重大信息安全事件的发生所做的准备以及在事件发生后所采取的措施。

应急响应计划（Emergency Response Plan），是指在突发/重大信息安全事件后对包括计算机运行在内的业务运行进行维持或恢复的策略和规程。信息安全应急响应计划的制定是一个周而复始、持续改进的过程，包含以下几个阶段：

（1）应急响应需求分析和应急响应策略的确定。

（2）编制应急响应计划文档。

(3) 应急响应计划的测试、培训、演练和维护。

4.2.2 我国信息安全事件应急响应工作的进展情况和政策要求

1. 我国信息安全事件应急响应工作的进展情况

与美国第一个应急组织诞生的原因类似,我国应急体系的建立也是由于网络蠕虫事件的发生而开始,这次蠕虫事件就是发生在 2001 年 8 月的红色代码蠕虫事件。由于红色代码集蠕虫、病毒和木马等攻击手段于一身,利用 Windows 操作系统一个公开漏洞作为突破口,几乎是畅通无阻地在互联网上疯狂地扩散和传播,迅速传播到我国互联网,并很快渗透到金融、交通、公安、教育等专用网络中,造成互联网运行速度急剧下降,局部网络甚至一度瘫痪。

当时我国仅有几个力量薄弱的应急组织,根本不具备处理如此大规模事件的能力,而各互联网运维部门也没有专门的网络安全技术人员,更没有互相协同处理的机制,各方几乎都束手无策。紧要关头,在 CNCERT/CC 的建议下,信息产业部组织了各个互联网单位和网络安全企业参加的应急响应会,汇总了全国当时受影响的情况,约定了协调处理的临时机制,确定了联系方式,并最终组成了一个网络安全应急处理联盟。

2001 年 10 月,信息产业部提出建立国家计算机紧急响应体系,并且要求各互联网运营单位成立紧急响应组织,能够加强合作、统一协调、互相配合。自此,我国的应急体系应运而生。目前,我国应急处理体系已经经历了从点状到树状的发展过程,并正在朝网状发展完善,最终要建设成一个覆盖全国全网的应急体系。

我国当前的网络应急组织体系是在国家网络与信息安全协调小组办公室领导下建设的,分为国家级政府层次、国家级非政府层次和地方级非政府层次等 3 个层面。

国家级政府层次由信息产业部互联网应急处理协调办公室为中心,向下领导国家级非政府层次的工作,横向与我国其他部委之间进行协调联系,同时负责与国外同层次的政府部门(如 APEC 经济体)之间进行交流和联系。

国家级非政府层次以 CNCERT/CC 为中心,向上接受信息产业部的领导,向下领导其遍布全国各省的分中心的工作,协调各个骨干互联网单位 CERT 小组的应急处理工作,协调和指导国家计算机病毒应急处理中心、国家计算机网络入侵防范中心和国家 863 计划反计算机入侵和防病毒研究中心等 3 个专业应急组织的工作,指导公共互联网应急处理国家级试点单位的应急处理工作;CNCERT/CC 同时还负责与国际民间 CERT 组织之间的交流和联系,负责利用自身的网络安全监测平台对全国互联网的安全状况进行实时监测。在这个层次中,还有正在建设中的信息产业部网络安全、信息安全和应急处理等 3 个专业的重点实验室,其任务是进行专门的技术研究,为 CNCERT/CC 开展应急处理协调工作提供必要的技术支撑。

地方级非政府层次主要以 CNCERT/CC 各省分中心为中心,协调当地的 IDC 应急组织、指导公共互联网应急处理服务省级试点单位开展面向地方的应急处理工作。

整个体系由国家网络与信息安全协调小组、信息产业部、CNCERT/CC 及其各省分中心构成核心框架,协调和指导各互联网单位应急组织、专业应急组织、安全服务试点单位和地方 IDC 应急组织共同开展工作,各自明确职责和工作流程,形成了一个有机的整体。

CNCERT/CC 成立于 2000 年 10 月,主要职责是协调我国各计算机网络安全事件应急小组,共同处理国家公共电信基础网络上的安全紧急事件,为国家公共电信基础网络、国家

主要网络信息应用系统以及关键部门提供计算机网络安全的监测、预警、应急、防范等安全服务和技术支持，及时收集、核实、汇总、发布有关互联网安全的权威性信息，组织国内计算机网络安全应急组织进行国际合作和交流。

其从事的工作内容包括如下：

（1）信息获取。通过各种信息渠道与合作体系，及时获取各种安全事件与安全技术的相关信息。

（2）事件监测。及时发现各类重大安全隐患与安全事件，向有关部门发出预警信息，提供技术支持。

（3）事件处理。协调国内各应急小组处理公共互联网上的各类重大安全事件，同时，作为国际上与中国进行安全事件协调处理的主要接口，协调处理来自国内外的安全事件投诉。

（4）数据分析。对各类安全事件的有关数据进行综合分析，形成权威的数据分析报告。

（5）资源建设。收集整理安全漏洞、补丁、攻击防御工具、最新网络安全技术等各种基础信息资源，为各方面的相关工作提供支持。

（6）安全研究。跟踪研究各种安全问题和技术，为安全防护和应急处理提供技术和理论基础。

（7）安全培训。进行网络安全应急处理技术及应急组织建设等方面的培训。

（8）技术咨询。提供安全事件处理的各类技术咨询。

（9）国际交流。组织国内计算机网络安全应急组织进行国际合作与交流。

CNCERT/CC 应急处理案例包括：网络蠕虫事件，如 SQL Slammer 蠕虫、口令蠕虫、冲击波蠕虫等；DDOS 攻击事件，部分政府网站和大型商业网站遭到了攻击；网页篡改事件，全国共有 435 台主机上的网页遭到篡改，其中包括 143 个主机上的 337 个政府网站在内；网络欺诈事件，处理了澳大利亚和中国香港等 CERT 组织报告的几起冒充金融网站的事件。

2. 我国信息安全事件应急响应工作政策要求

国家信息安全保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

国家有关政策规定的加强信息安全保障工作，主要遵循下述原则：

（1）基于安全需求原则。组织机构应根据其信息系统担负的使命，积累的信息资产的重要性，可能受到的威胁及面临的风险分析安全需求，按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，从全局上恰当地平衡安全投入与效果。

（2）主要领导负责原则。主要领导应确立其组织统一的信息安全保障的宗旨和政策，负责提高员工的安全意识，组织有效安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效。

（3）全员参与原则。信息系统所有相关人员应普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全。

（4）系统方法原则。按照系统工程的要求，识别和理解信息安全保障相互关联的层面和过程，采用管理和技术结合的方法，提高实现安全保障的目标的有效性和效率。

（5）持续改进原则。安全管理是一种动态反馈过程，贯穿整个安全管理的生存周期，随

着安全需求和系统脆弱性的时空分布变化，威胁程度的提高、系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性。

（6）依法管理原则。信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响。

（7）分权和授权原则。对特定职能或责任领域的管理功能实施分离、独立审计等实行分权，避免权力过分集中所带来的隐患，以减小未授权的修改或滥用系统资源的机会。任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必需的权限，不应享有任何多余权限。

（8）选用成熟技术原则。成熟的技术具有较好的可靠性和稳定性，采用新技术时要重视其成熟的程度，并应首先局部试点然后逐步推广，以减少或避免可能出现的失误。

（9）分级保护原则。按等级划分标准确定信息系统的安全保护等级，实行分级保护；对多个子系统构成的大型信息系统，确定系统的基本安全保护等级，并根据实际安全需求，分别确定各子系统的安全保护等级，实行多级安全保护。

（10）管理与技术并重原则。坚持积极防御和综合防范，全面提高信息系统安全防护能力，立足国情，采用管理与技术相结合，管理科学性和技术前瞻性相结合的方法，保障信息系统的安全性达到所要求的目标。

（11）自保护和国家监管结合原则。对信息系统安全实行自我保护和国家保护相结合。组织机构要对自己的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护能力和水平，保障国家信息安全。

《关于加强信息安全保障工作的意见》（中办发[2003]27 号文）指出："信息安全保障工作的要点在于，实行信息安全等级保护制度，建设基于密码技术的网络信任体系，建设信息安全监控体系，重视信息安全应急处理工作，推动信息安全技术研发与产业发展，建设信息安全法制与标准"。国家信息安全战略的近期目标：通过 5 年的努力，基本建成国家信息安全保障体系。

对于信息安全事件的应急响应，国家发布了以下标准：《信息安全技术信息安全应急响应计划规范》（GB/T 24364—2009）、《信息安全技术信息系统灾难恢复规范》（GB/T 20988—2007）、《信息技术 安全技术 信息安全事件管理指南》（GB/Z 20985—2007）、《信息安全技术 信息安全事件分类分级指南》（GB/Z 20986—2007）。

4.2.3 信息安全应急响应阶段方法论

1. 应急响应六阶段

（1）准备阶段，要严阵以待。在该阶段要做到：

① 预防为主。

② 微观（一般观点）。帮助服务对象建立安全政策，按照安全政策配置安全设备和软件，进行扫描和风险分析，及时打补丁，如有条件且得到许可，应该建立监控设施。

③ 宏观。建立协作体系和应急制度以及信息沟通渠道和通报机制，如有条件，还应该

建立数据汇总分析的体系和能力,需要制订有关法律法规。

④ 制定应急响应计划。

⑤ 资源准备。需要准备的资源主要包括应急经费筹集、人力资源、软硬件设备、现场备份、业务连续性保障、系统容灾、搭建临时业务系统等。

(2) 确认阶段,是对情况的综合判断。在该阶段要做到:

① 确定事件性质和处理人。

② 微观(负责具体网络的CERT)。确定事件的责任人:指定一个责任人全权处理此事件;给予必要的资源。

确定事件的性质:误会、玩笑、还是恶意的攻击/入侵;影响的严重程度;预计采用什么样的专用资源来修复。

③ 宏观(负责总体网络的CERT)。通过汇总,确定是否发生了全网的大规模事件,确定应急等级,以决定启动哪一级应急方案。

(3) 遏制阶段,要制止事态的扩大。故该阶段应该做到:

① 即时采取的行动。

② 微观。防止进一步的损失,确定后果。进行初步分析,重点是确定适当的封锁方法,咨询安全政策,确定进一步操作的风险,将损失降到最小化(以最快、最简单的方式恢复系统的基本功能,如备机启动),可列出若干选项,讲明各自的风险,由服务对象选择。

③ 宏观。要确保封锁方法对各网业务的影响最小,通过协调争取各网一致行动,实施隔离,汇总数据,估算损失和隔离效果。

(4) 根除阶段,要找到彻底的补救措施,在该阶段需要做到:

① 寻找长期的补救措施。

② 微观。进行详细分析,确定原因,定义征兆,分析漏洞,同时加强防范,消除原因,修改安全政策。

③ 宏观。加强宣传,公布危害性和解决办法,呼吁用户解决终端的问题;加强检测工作,发现和清理行业与重点部门的问题。

(5) 恢复阶段,在此阶段系统要恢复常态,包括以下两个方面:

① 微观。被攻击的系统恢复正常的工作状态,作一个新的备份,把所有安全上的变更作备份,重新上线服务,持续监控。

② 宏观。持续汇总分析,了解各网的运行情况,要根据各网的运行情况判断隔离措施的有效性,通过汇总分析的结果判断仍然受影响的终端的规模,发现重要用户应该及时通报解决,在适当的时候解除封锁措施。

(6) 跟踪阶段,在该阶段主要考虑的问题为:还会有第二次吗?在跟踪过程中应该做到:

① 关注系统恢复以后的安全状况,特别是曾经出问题的地方。

② 建立跟踪文档,规范记录跟踪结果。

③ 对响应效果给出评估。

④ 对进入司法程序的事件,做进一步的调查,打击违法犯罪活动。

2. 事件的归档与统计

对所处理的信息安全应急响应事件应该及时归档和统计。事件的归档应该包括以下几

点必需的内容：如处理人、时间和时段、地点、工作量、事件的类型、对事件的处置情况、代价、细节等。

4.2.4 信息安全应急响应计划编制方法

具体的组织体系结构及人员职责；应急响应计划各小组成员的联络信息；供应商联络信息，包括离站存储和备用站点的外部联系点；系统恢复或处理的标准操作规程和检查列表；支持系统运行所需的硬件、软件、固件和其他资源的设备和系统需求清单；供应商服务水平协议(SLA)、与其他机构的互惠协议和其他关键记录；备用站点的描述和说明；在计划制定前进行的 BIA，包含关于系统各部分相互关系、风险、优先级别等；应急响应计划文档的保存和分发方法。

4.2.5 应急响应小组的作用和建立方法

1. 应急响应工作结构

组织应结合本单位日常机构建立信息安全应急响应的工作机构，并明确其职责。其中一些人可负责两种或多种职责，一些职位可由多人担任(应急响应计划文档中应明确他们的替代顺序)。

应急响应的工作机构由管理、业务、技术和行政后勤等人员组成。一般来说，按角色可划分为 5 个功能小组，即应急响应领导小组、应急响应技术保障小组、应急响应专家小组、应急响应实施小组和应急响应日常运行小组等。各小组工作结构及职能如图 4.4 所示。

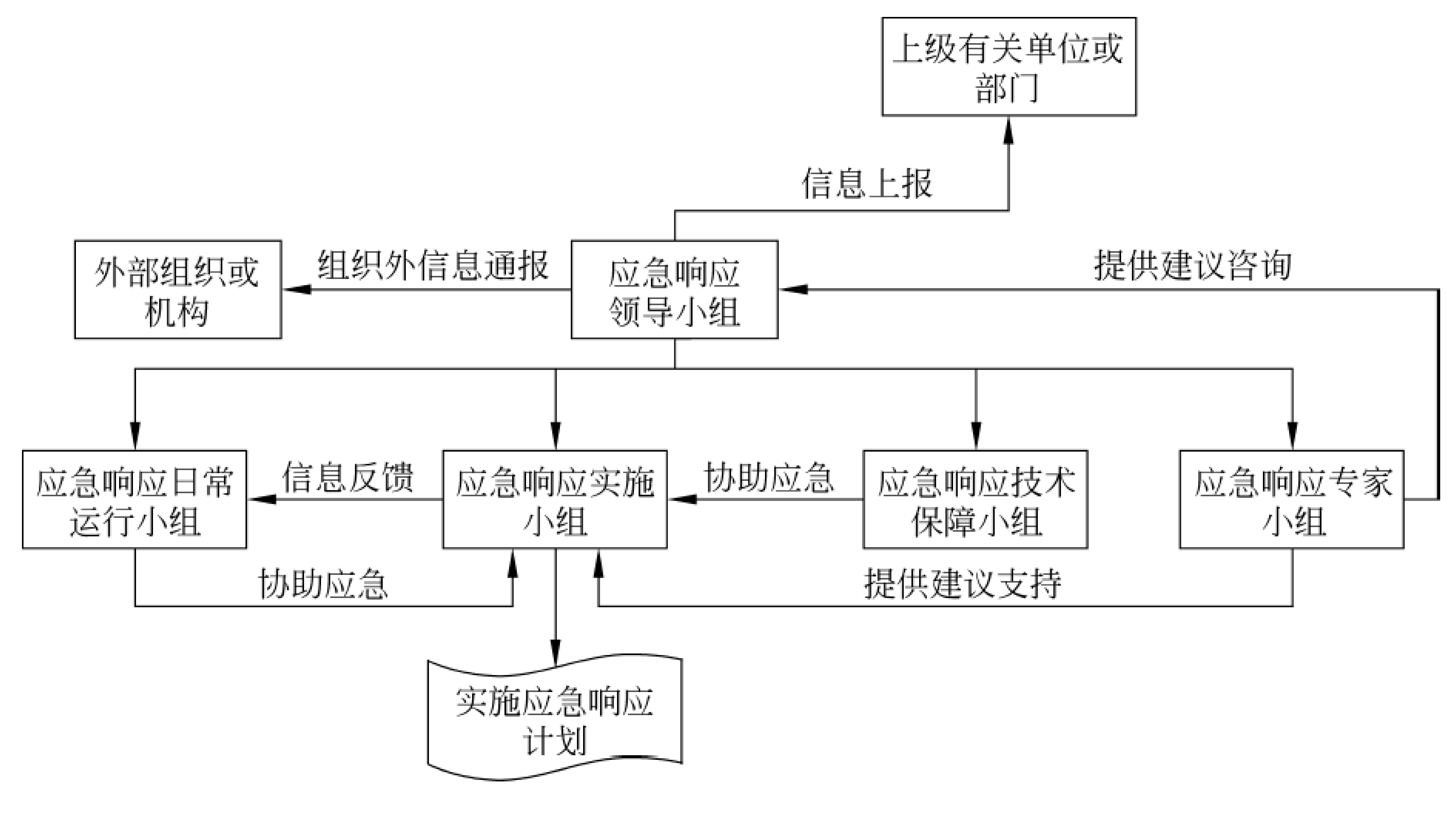


图 4.4 应急响应工作结构

实际中，可以不必专门成立对应的功能小组，组织可以根据自身情况由其具体的某个或某几个部门或部门中的某几个人担当其中的一个或几个角色。组织可聘请具有相应资质的外部专家协助应急响应工作，也可委托具有相应资质的外部机构承担实施小组以及日常运行小组的部分或全部工作。在聘请外部专家协助应急响应工作或者委托外部机构承担部分或者全部应急响应工作时需要和其签订相关协议(如签订有关信息保密要求等)。

2. 职责示例

1）应急响应领导小组

应急响应领导小组是信息安全应急响应工作的组织领导机构，组长应由组织最高管理层成员担任。领导小组的职责是领导和决策信息安全应急响应的重大事宜，主要包括如下：

（1）对应急响应工作的承诺和支持，包括发布正式文件、提供必要资源（人财物）等。

（2）审核并批准应急响应策略。

（3）审核并批准应急响应计划。

（4）批准和监督应急响应计划的执行。

（5）启动定期评审、修订应急响应计划。

（6）负责组织的外部协作工作。

2）应急响应技术保障小组

应急响应技术保障小组的主要职责包括如下：

（1）制定信息安全事件技术应对表。

（2）制定信息安全事件区域技术应对表。

（3）制定具体角色和职责分工细则。

（4）制定应急响应协同调度方案。

（5）考察和管理相关技术基础。

3）应急响应专家小组

应急响应专家小组的主要职责包括如下：

（1）对重大信息安全事件进行评估，提出启动应急响应级别的建议。

（2）研究分析信息安全事件的相关情况及发展趋势，为应急响应提供咨询或提出建议。

（3）分析信息安全事件原因及造成的危害，为应急响应提供技术支持。

4）应急响应实施小组

应急响应实施小组的主要职责包括如下：

（1）分析应急响应需求，如风险评估、业务影响分析等。

（2）确定应急响应策略和等级。

（3）实现应急响应策略。

（4）编制应急响应计划文档。

（5）实施应急响应计划。

（6）组织应急响应计划的测试、培训和演练。

（7）合理部署和使用应急响应资源。

（8）总结应急响应工作，提交应急响应总结报告。

（9）执行应急响应计划的评审、修订任务。

5）应急响应日常运行小组

应急响应日常运行小组的主要职责包括如下：

（1）协助灾难恢复系统实施。

（2）备份中心日常管理。

（3）备份系统的运行和维护。

(4) 应急监控系统的运作和维护。

(5) 参与和协助应急响应计划的测试、培训和演练。

(6) 维护和管理应急响应计划文档。

(7) 信息安全事件发生时的损失控制和损害评估。

4.2.6 我国信息安全事件分级分类方法

根据《信息安全事件分级分类指南》(GB/Z 20986—2007)将信息安全事件划分为：有害程序事件；网络攻击事件；信息破坏事件；信息内容安全事件；设备设施故障、灾害性事件；其他信息安全事件。

我国信息安全事件按照系统损失、社会影响、信息系统的重要程度3个分级要素分为特别重大事件、重大事件、较大事件和一般事件。分级要素如图4.5所示。

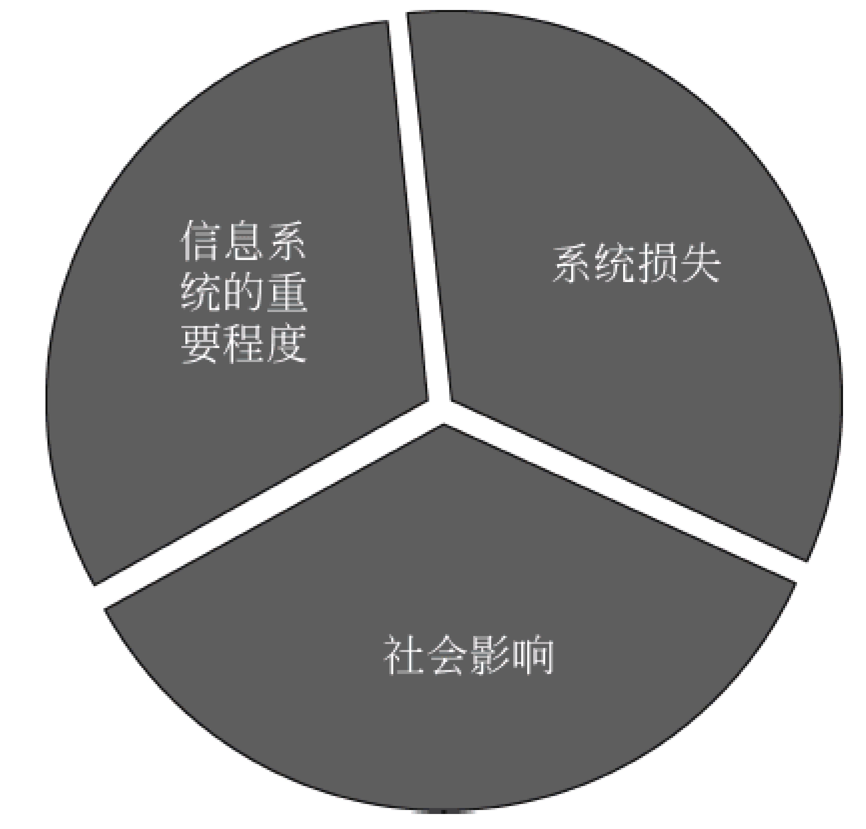


图4.5　分级要素

特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：会使特别重要信息系统遭受特别严重的系统损失；产生特别重大的社会影响。

重大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况：会使特别重要信息系统遭受严重的系统损失或使重要信息系统遭受特别严重的系统损失；产生重大的社会影响。

较大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况：会使特别重要信息系统遭受较大的系统损失或使重要信息系统遭受严重的系统损失，一般信息系统遭受特别严重的系统损失；产生较大的社会影响。

一般事件是指不满足以上条件的信息安全事件，包括以下情况：会使特别重要信息系统遭受较小的系统损失或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失；产生一般的社会影响。

4.2.7 国际和我国信息安全应急响应组织

1. 国际信息安全应急响应组织

国际信息安全应急响应组织有：美国计算机紧急事件响应小组协调中心(Computer Emergency Response Team/Coordination Center，CERT/CC)；事件响应与安全组织论坛(Forum of Incident Response and Security Teams，FIRST)；亚太地区计算机应急响应组织(Asia Pacific Computer Emergency Response Team，APCERT)；欧洲计算机网络研究教育协会(Trans-European Research and Education Networking Association，TERENA)。

2. 我国信息安全应急响应组织

我国的信息安全应急响应组织有：国家计算机网络应急技术处理协调中心(National Computer network Emergency Response technical Team/Coordination Center of China，CNCERT/CC)；中国教育和科研计算机网络紧急响应组织(China Education and Research

Network Computer Emergency Response Team,CCERT);国家计算机病毒应急处理中心;国家计算机网络入侵防范中心;国家863计划反计算机入侵和防病毒研究中心。

4.2.8 计算机取证的概念和作用

1. 背景

随着社会信息化、网络化大潮的推进,社会生活中的计算机犯罪层出不穷。信息技术发展对法律体系的挑战,超出以往任何一次技术变革所带来的冲击,如国家安全问题、电信基础网络安全问题、金融系统安全问题、知识产权问题、网络诈骗问题、IP电话问题、黄色泛滥问题等。电子数据证据的法律效力正在成为学术界关注的焦点。

要解决这些问题,既要面对法律层面的挑战,也要迎接技术层面的挑战。

2. 计算机犯罪的概念及特点

广义地说,计算机犯罪通常是指所有涉及计算机的犯罪。例如,欧洲经济合作与发展组织的专家认为:“在自动数据处理过程中任何非法的、违反职业道德的、未经过批准的行为都是计算机犯罪”。我国刑法学者有人认为:“凡是故意或过失不当使用计算机致使他人受损失或有受损失危险的行为,都是计算机犯罪”。

狭义地说,计算机犯罪通常是对计算机资产本身进行侵犯的犯罪。例如,瑞典的私人保密权法规:“未经过批准建立和保存计算机私人文件,非法窃取电子数据处理记录或非法篡改、删除记录侵犯个人隐私的行为都是计算机犯罪。”我国有学者认为,“计算机犯罪是指利用计算机操作所实施的危害计算机信息系统(包括内存数据及程序)安全的犯罪行为。”

折中地说,计算机本身在计算机犯罪中以“犯罪工具”或“犯罪对象”的方式出现,这一概念注重的是计算机本身在犯罪中的作用。例如,德国学者施奈德认为:“计算机犯罪指的是利用电子数据处理设备作为作案工具的犯罪行为或者把数据处理设备当作作案对象的犯罪行为。”我国学者认为:“计算机犯罪是以计算机为工具或以计算机资产为对象的犯罪行为。”

计算机犯罪特点如下。

(1) 犯罪形式的隐蔽性。计算机犯罪一般不受时间和地点限制,可以通过网络大幅度跨地域远程实现,其罪源可来自全球的任何一个终端,随机性很强。

(2) 犯罪主体和手段的智能性。计算机犯罪的各种手段中,无论是“特洛伊木马术”还是“逻辑炸弹”,无一不是凭借高科技手段实施的,犯罪嫌疑人具有相当丰富的计算机技术知识和娴熟的计算机操作技能。

(3) 跨国性。网络冲破了地域限制,计算机犯罪呈国际化趋势。因特网具有“时空压缩化”的特点,这为犯罪分子跨地域、跨国界作案提供了可能。犯罪分子只要拥有一台联网的终端机,就可以通过因特网到网络上任何一个站点实施犯罪活动。由于这种跨国界、跨地区的作案隐蔽性强、不易侦破,危害也就更大。

(4) 匿名性。罪犯在接受网络中的文字或图像信息的过程是不需要任何登记的,完全匿名,因而对其实施的犯罪行为也就很难控制。

(5) 损失大,对象广泛,发展迅速,涉及面广。我国从1986年开始每年出现至少几起或几十起计算机犯罪,到1993年一年就发生了上百起,近几年利用计算机犯罪的案件以每年30%的速度递增,每年造成的直接经济损失近亿元。

(6) 持获利和探秘动机居多。全世界每年被计算机犯罪直接盗走的资金达 20 亿美元。我国 2001 年发现的计算机作案的经济犯罪已达 100 余件，涉及金额达 1700 万元，在整个计算机犯罪中占有相当大的比例。各种各样的个人隐私、商业秘密、军事秘密等都成为计算机犯罪的攻击对象。侵害计算机信息系统的更是层出不穷。

(7) 低龄化和内部人员多。我国对某地的金融犯罪情况的调查，犯罪年龄在 35 岁以下的人占整个犯罪人数的比例在 70%左右。其中年龄最小的只有 18 岁。在计算机犯罪中犯罪主体中内部人员也占有相当大的比例。据有关统计，计算机犯罪的主体在金融、证券业中内部人员犯罪的占 78%。

(8) 巨大的社会危害性。网络的普及程度越高，计算机犯罪的危害也就越大，而且计算机犯罪的危害性远非一般传统犯罪所能比拟，不仅会造成财产损失，而且可能危及公共安全和国家安全。据美国联邦调查局统计测算，一起刑事案件的平均损失仅为 2000 美元，而一起计算机犯罪案件的平均损失高达 50 万美元。据计算机安全专家估算，近年因计算机犯罪给总部在美国的公司带来的损失为 2500 亿美元。

计算机犯罪如非法侵入计算机信息系统罪：《中华人民共和国刑法》第 285 条规定，违反国家规定，侵入国有事务、国防建设、尖端科学技术领域的计算机信息系统的，处 3 年以下有期徒刑或者拘役。破坏计算机信息系统罪：《中华人民共和国刑法》第 286 条概括为破坏计算机信息系统罪，主要表现为：故意对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的行为；故意对计算机信息系统中存储处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的行为；故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的行为。

3. 计算机取证的概念

1) 计算机取证的概念

计算机取证是指对能够为法庭接受的、足够可靠和有说服力的，存在于计算机和相关外设中的电子证据的确认、保护、提取和归档的过程。

计算机取证技术就是打击信息技术犯罪的一项有效手段。该技术将计算机系统视为犯罪工具或现场，运用先进的技术手段，按照规程全面检查计算机系统，提取、保护并分析与计算机犯罪相关的证据，并据此提起诉讼。

2) 计算机证据的重要性

计算机证据在计算机屏幕上的表现形式具有多样性，尤其是多媒体技术的出现，更使这些证据综合了文本、图形、图像、动画、音频及视频等多种形式，这种以多媒体形式存在的计算机证据几乎涵盖了所有的传统证据类型，如电子物证、电子书证、电子视听资料、电子证人证言、电子当事人陈述、关于电子证据的鉴定结论以及电子勘验检查笔录等。

很多案件本身不涉及计算机系统，但却是通过计算机系统破案的。

我国学者何家弘先生对电子证据做过一个断言："就司法证明方法的历史而言，人类曾经从神证时代走入人证时代；又从人证时代走入物证时代。也许，我们即将走入另一个新的司法证明时代，即电子证据时代。"这句话并不是说，电子证据将取代一切传统证据，但信息时代，电子证据不可避免地被一些专家誉为"证据之王"。

在作为证据的共同要求方面，计算机证据与传统证据一样，必须可信、准确、完整、符合法律法规，即可为法庭所接受。

由于计算机证据所具有的特殊性，如何对其进行收集、保护、分析和展示，成了司法和计算机科学领域新的研究课题。

3）计算机证据与传统证据的区别

计算机证据与传统证据的最大区别就在于其脆弱性、易毁性、隐蔽性及非直观性。不借助一定的环境，这些证据似乎是看不见、摸不着的。传统证据如文书，可以直接观察，然后才是不容易改变，或者改变后会或多或少留下痕迹。然而计算机证据往往更难以获取，给人一种不可捉摸，尤其是无法把握、危险万分的印象。

计算机系统相关的犯罪案例中可以扮演黑客入侵的目标、作案的工具和犯罪信息的存储器3种角色。无论作为哪种角色，计算机及其外设中都会留下大量与犯罪有关的证据。对其进行获取、保存、分析和出示，其技术实质就是对计算机系统进行处理，得到相关数据，从而重建其犯罪过程。取证人员必须设法保存尽可能多的犯罪信息。犯罪的证据可能存在于系统日志、数据文件、存储器、交换区、隐藏文件、空闲的磁盘空间、打印机缓存、网络数据区和计数器、用户进程存储区、堆栈、文件缓冲区、文件系统本身等不同的位置。

4. 计算机证据获取的一般步骤

计算机证据的获取一般分为两大步骤：第一步是实体物理设备或软件系统的获取，即计算机系统的获取；第二步是证据分析。

物理证据获取是全部取证工作的基础，在获取物理证据时最重要的工作是保证获取的原始证据不受到任何破坏，无论在何种情况下，调查者都必须牢记以下几点：

（1）不改变原始记录。

（2）不在作为证据的计算机上执行无关的程序。

（3）不给犯罪者销毁证据的机会。

（4）详细记录所有的取证活动。

（5）妥善保存得到的物证。

获取物理证据后，接下来的工作就是信息发现。不同的案例对信息发现的要求是不一样的，在有些情况下，只需找到关键的文件、图片或邮件就可以了，在其他时候则可能要求重现计算机在过去工作的细节，如入侵取证。

为了保护原始数据，除非有特殊的需要，所有信息发现工作都是对原始证据的物理副本进行的，所有的工作都是可重复验证的。

一般情况下，取证人员还要用算法（MD5）对原始证据上的数据做摘要，然后把原始证据和摘要信息及相关文档妥善保存。

最后，取证人员会就计算机信息发现的结果做出完整的报告，这个报告将成为打击犯罪者的依据。

5. 计算机取证的分类

计算机取证一般分为两大类。

一类是有准备的取证，称之为有预谋的取证，这种取证的最大特点是周期较长，并具有主动性、计划性和针对性。常常是发现了蛛丝马迹后，主动采取一些技术手段，进行监视和跟踪。

另一类是事后调查取证，通常具有盲目性，或只有一般线索，并不能确定获取的物理证物中一定就能找到证据。

按应用环境，计算机取证分为两大类。

单机环境取证是指对不联网机器的取证调查。这类应用往往是一次性的、突击性的。例如，调查时获取相应的计算机或物理存储设备，然后对其进行分析，查找相应的证据，更多的应用是事后取证。

网络环境取证更容易采取主动取证手段，如网络监控、网络抓帧，通过服务器或代理服务器记录嫌疑人计算机所有的网络活动，或采用合法的类似于黑客的技术手段等，对重点目标进行24h的监控等。

计算机取证的初步流程如图4.6所示。

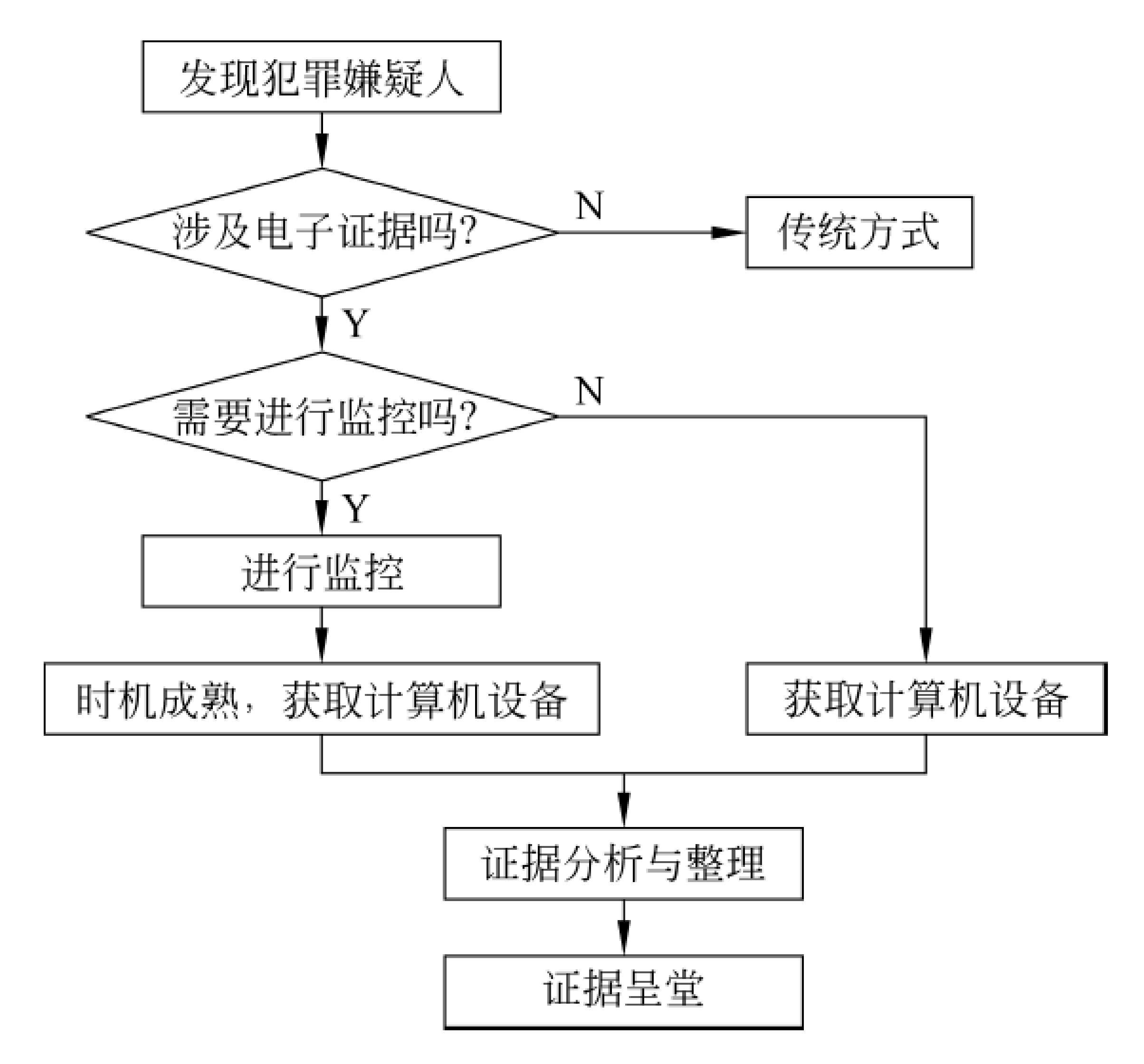


图4.6 计算机取证的初步流程

6. 证据分析的技术体系

证据分析是一项技术性很强的复杂工作。例如，犯罪嫌疑人用于记录非法交易的Word文档，如果被删除，可以通过技术手段将该文档完整地恢复回来，那么得到的信息就是一个完整的信息，就能够得到其交易记录。这个文档已经部分遭到破坏，不能够完整恢复，这时就需要分析磁盘，分析该文件，尽可能多地恢复其中的内容。

取证工作的层次性很强，可以分层次地分析与获取。一般而言，取证工作分为以下几层：

(1) 网络层，通过网络技术获取证据。本层次主要应用于主动取证，如在犯罪嫌疑人不知不觉的情况下，通过高速网络抓帧技术，得到犯罪嫌疑人所有进出网络的数据，进而重现其所有的网络活动；或者通过在路由器、服务器或代理服务器等必经地进行设置，得到其所有网络活动记录。

(2) 网络存储层，指通过网络存储层获取证据。该层次针对存储子系统。直接附加存储(DAS)数据存储是整个服务器结构的一部分，这种情况下的数据和操作系统往往是不分离的。所以，很多时候的取证工作需要将操作系统与存储系统结合起来进行分析。在存储区域网络(SAN)中，存储设备通过专用交换机连接到一群计算机上，在该网络中提供了多主机连接，允许任何服务器连接到任何存储阵列，让多主机访问存储器和主机间访问一样方

便，这样不管数据放置在哪里，服务器都可直接存取所需的数据。网络附加存储（NAS）设备提供 RJ-45 接口和单独的 IP 地址，可以将其直接挂接在主干网的交换机或其他局域网的 Hub 上，通过简单的设置（如设置机器的 IP 地址等）就可以在网络即插即用地使用 NAS 设备。鉴于 NAS 的特点，其取证工作会更加复杂一些，不仅要从操作系统中提取数据，还需要从存储系统中提取数据，并且由于多机对一个 NAS 系统，还需要分析数据的隶属关系。

（3）磁盘阵列层。在该层次上，主要是解决阵列架、阵列卡损坏、磁盘掉线等故障，如果要搜查的证据分布在多个磁盘上，对单个磁盘搜索是没有任何意义的，必须重建 RAID 才能够得到有用的证据。

（4）磁盘级。犯罪分子有时候会采取破坏设备，如破坏计算机或硬盘的方式，以防止硬盘中的犯罪信息被提取出来，以达到销毁证据的目的。

（5）文件系统级。在文件系统损坏的情况下去搜索关键字显然是没有意义的，只有恢复完整的文件，才是查找证据最好的解决之道。比如，仅仅分区表损坏，将分区表重建一下，系统就完全回到正常状态，所有的文件都可以正常访问，而如果教条地用搜索关键字的方法，直接对磁盘进行搜索，显然是得不到有效数据的，效率也极其低下。

（6）文件级。文件级包含了多种情况，如很多时候，文件系统损坏得比较严重，恢复的效果不是很理想。这时就需要对这些文件格式有所了解，如一个受损的 Word 文档，用程序是无法正常打开显示其内容的，但可能只是文件头部分损坏，里面含有大量信息的文字并没有丢失，就可以通过技术手段，将文字信息提取出来。加密与解密、信息隐藏等更是取证中需要解决的问题，如将信息隐藏在图片中，不知底细的人，只能看到正常的图片，根本无法发现和查看图片中隐藏的秘密信息。所以，文件级是差别最大、应用最复杂、需要解决问题最多的级别。

所有这些级别基本只是针对信息流和存储系统而言的，事实上，取证工作与操作系统是密切相关、不可分割的。

犯罪信息本身，就有很多散布在操作系统的信息中，如注册表、虚拟内存、系统日志、缓存等处，并且还要熟悉操作系统后台会进行什么操作，以方便重建犯罪现场。

7. 展望

作为一门新兴的交叉学科，计算机取证技术还需要更多的人来投入其中进行深入研究和分析。目前的计算机取证技术尚处于发展初期，既有未解决的技术问题，更有未解决的法律问题，需要各方面的相关人员共同努力，来促进其健康、有序、有效地协调发展。

计算机取证技术热点问题主要有：数据获取技术；数据分析技术；数据恢复技术；取证和证据分析工具的开发；往往结合人工智能、机器学习、神经网络和数据挖掘技术。下面对主要关键技术做详细介绍。

（1）数据获取技术。对计算机系统和文件的安全获取技术，避免对原始介质进行任何破坏和干扰；对数据和软件的安全搜集技术；对磁盘或其他存储介质的安全无损伤备份技术；对已删除文件的恢复、重建技术；对磁盘空间、未分配空间和自由空间中包含的信息的发掘技术；对交换文件、缓存文件、临时文件中包含的信息的复原技术；计算机在某一特定时刻活动内存中的数据的搜集技术；网络流动数据的获取技术等。

（2）数据分析技术。在已经获取的数据流或信息流中寻找、匹配关键词或关键短语是目前的主要数据分析技术；文件属性分析技术；文件数字摘要分析技术；日志分析技术；根据

已经获得的文件或数据的用词、语法和写作(编程)风格,推断出其可能的作者的分析技术;发掘同一事件的不同证据间的联系的分析技术;数据解密技术;密码破译技术;对电子介质中的被保护信息的强行访问技术等。

(3) 数据恢复技术。文件被删除时的恢复;文件损坏时的恢复;硬盘被加密或变换时的恢复;加密文件后密码破解;缺乏用户口令进入文件系统方法;格式化后硬盘数据的恢复。

对于法律的问题,世界各国有的将传统法加以延伸,使之适用于电子证据领域,有的针对电子证据专门制定相应的电子法律。我国目前正在着手制定证据法。相信随着法律体系的完善,电子证据或者计算机证据,一定会在打击各种犯罪活动方面发挥其应有的作用。

计算机取证科学,是一门技术性非常强的边缘学科,其任何工作都必须有严格的控制程序,所得结果必须经得住考验,并可以反复验证确认,要求其操作和结果都建立在网络和文件系统的基础之上,尽量获取完整、可信的信息。

4.2.9 计算机取证的原则、基本步骤、常用方法和工具

1. 计算机取证的原则

计算机取证的主要原则有以下几点:

(1) 尽早搜集证据,并保证其没有受到任何破坏。

(2) 必须保证“证据连续性”(有时也被称为 Chain of Custody),即在证据被正式提交给法庭时,必须能够说明在证据从最初的获取状态到在法庭上出现状态之间的任何变化,当然最好是没有任何变化。

(3) 整个检查、取证过程必须是受到监督的,也就是说,由原告委派的专家所做的所有调查取证工作,都应该受到由其他方委派的专家的监督。

2. 计算机取证的基本步骤

在保证以上几项基本原则的情况下,计算机取证工作一般按照下面步骤进行:

(1) 在取证检查中,保护目标计算机系统,避免发生任何的改变、伤害、数据破坏或病毒感染。

(2) 搜索目标系统中的所有文件,包括现存的正常文件、已经被删除但仍存在于磁盘上(即还没有被新文件覆盖)的文件、隐藏文件、受到密码保护的文件和加密文件。

(3) 全部(或尽可能)恢复发现的已删除文件。

(4) 最大程度地显示操作系统或应用程序使用的隐藏文件、临时文件和交换文件的内容。

(5) 如果可能并且法律允许,访问被保护或加密文件的内容。

(6) 分析在磁盘的特殊区域中发现的所有相关数据。特殊区域至少包括下面两类:未分配磁盘空间——虽然目前没有被使用,但可能包含有先前的数据残留;文件中的 Slack 空间——如果文件的长度不是簇长度的整数倍,那么分配给文件的最后一簇中,会有未被当前文件使用的剩余空间,其中可能包含了先前文件遗留下来的信息,可能是有用的证据。

(7) 打印对目标计算机系统的全面分析结果,然后给出分析结论。系统的整体情况,发现的文件结构、数据和作者的信息,对信息的任何隐藏、删除、保护、加密企图以及在调查中发现的其他相关信息。

(8) 给出必需的专家证明。

上面提到的计算机取证原则及步骤都是基于一种静态的视点，即事件发生后对目标系统的静态分析。随着计算机犯罪技术手段的提高，这种静态的视点已经无法满足要求，发展趋势是将计算机取证结合到入侵检测等网络安全工具和网络体系结构中，进行动态取证。整个取证过程将更加系统并具有智能性，也将更加灵活多样。

3. 计算机取证的常用方法和工具

计算机调查取证方式是目前的调查取证中新兴的技术模式，其在目前实践环境下得到相关调查机构的不断重视；计算机取证的方法就是计算机取证过程中涉及的具体措施、具体程序、具体方法。计算机取证的方法非常多，而且在计算机取证过程中通常又涉及证据的分析，取证与分析两者很难完全孤立开来，所以对计算机取证的分类十分复杂，往往难以按一定的标准进行合理分类。通常情况下根据取得证据的用途不同进行分类，通常可以分为两类不同性质的取证：一类是来源取证；另一类是事实取证。

（1）来源取证。来源取证，指的是取证的目的主要是确定犯罪嫌疑人或者证据的来源。例如，在网络犯罪侦查中，为了确定犯罪嫌疑人，可能需要找到犯罪嫌疑人犯罪时使用的机器的 IP 地址，则寻找 IP 地址便是来源取证。这类取证中，主要有 IP 地址取证、MAC 地址取证、电子邮件取证、软件账号取证等。

IP 地址取证主要是利用在互联网中，每一台联网的计算机，在某一时刻都有唯一的全局 IP 地址。根据在案发现场找到的 IP 地址信息，进一步确定犯罪嫌疑人的机器，由犯罪嫌疑人的机器再寻找案件相关人的方法。

MAC 地址取证主要在一些局域网中或动态分配 IP 地址网络中，由于 IP 地址使用有一定的自由，如果哪一个 IP 地址由谁租用并不清楚时，可以根据物理地址与逻辑地址的关系，找到物理地址，而物理地址也是唯一的，且一般情况下，也比较难以更改。所以 MAC 地址与特定计算机设备中网卡存在一定的对应关系，可以用来确定来源。

电子邮件取证，指的是根据电子邮件头部信息找到发送电子邮件的机器，并根据已锁定的机器找到特定人的取证方法。

软件账号取证，指特定软件如果其某个账号与特定人存在一一对应关系时，可以用来证明案件的来源。

（2）事实取证。事实取证指的是取证目的不是为了查明犯罪嫌疑人，而是取得与证明案件相关事实的证据，如犯罪嫌疑人的犯罪事实证据。在事实取证中常见的取证方法有文件内容调查、使用痕迹调查、软件功能分析、软件相似性分析、日志文件分析、网络状态分析、网络数据包分析等。

文件内容调查指的是在存储设备中取得文档文件、图片文件、音频视频文件、动画文件、网页、电子邮件内容等相关文件的内容。包括这些文件被删除以后、文件系统被格式化后或者数据恢复以后的文件内容。

使用痕迹调查包括 Windows 运行的痕迹（包括运行栏历史记录、搜索栏历史记录、打开/保存文件记录、临时文件夹、最近访问的文件等使用文件与程序调查）、上网记录的调查（缓存、历史记录、自动完成记录、浏览器地址栏下拉网址，Cookies、index. dat 文件等）、Office、Realplay 和 Mediaplay 的播放列表及其他应用软件使用历史记录。

软件功能分析主要针对特定软件和程序的性质和功能进行分析，常见的是对恶意代码的分析，确定其破坏性、传染性等特征。此类取证方法通常在破坏计算机信息系统、入侵计

算机信息系统、传播计算机病毒行为中经常使用。

软件相似性分析是指比较两软件，找出两者之间是否存在实质性相似的证据。此类取证方法主要在软件知识产权相关案件中使用。

日志文件分析指通过系统日志、数据库日志、网络日志、应用程序日志等进行分析发现系统是否存在入侵行为或者其他访问行为的证据。

网络状态分析指的是取得特定时刻计算机联网状态，如网络中哪些机器与本机相连、本机的网络配置、开启了哪些服务、哪些用户登录到本机等信息。

网络数据包分析指的是通过分析网络中传输的数据包发现相关证据的过程。网络数据包分析主要发生在实时取证中，是一种综合的取证方法。有时候网络数据包分析也称为“网络侦听”。在对网络犯罪实时侦查或“诱惑性”侦查时，往往采取网络侦听的方法发现犯罪嫌疑人的犯罪活动，掌握犯罪的线索，为抓获犯罪嫌疑人提供支持。

在常用的证据调查方法体系中，计算机取证作为一项新兴的调查取证方式，有着其极高的专业性和技术性，但一旦有所突破，也能获得较为明显的证据线索，有效地促进案件的证据整理工作，作为专业的证据调查部，要不断总结，掌握熟练的计算机取证技术，更好地为客户提供优质的证据服务。

计算机取证常用工具有 ENCASE X-WAYS FTK、DATACOMPASS 等工具。

4.3 业务连续性管理与灾难恢复

4.3.1 业务连续性管理与灾难恢复的基本概念

1. 灾难

灾难(Disaster)，《信息安全技术信息系统灾难恢复规范》(GB/T 20988—2007)中规定，是由于人为或自然的原因，造成信息系统严重故障或瘫痪，使信息系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。通常导致信息系统需要切换到灾难备份中心运行。典型的灾难事件包括：自然灾害，如火灾、洪水、地震、飓风、龙卷风、台风等；技术风险和提供给业务运营所需服务的中断，如设备故障、软件错误、通信网络中断和电力故障等；此外，人为的因素往往也会酿成大祸，如操作员错误、植入有害代码和恐怖袭击。

2. 业务连续性管理

业务连续性管理(Business Continuity Management，BCM)为保护组织的利益、声誉、品牌和价值创造活动，找出对组织有潜在影响的威胁，提供建设组织有效反应恢复能力的框架的整体管理过程，包括组织在面临灾难时对恢复或连续性的管理，以及为保证业务连续计划或灾难恢复预案的有效性的培训、演练和检查的全部过程。业务连续性管理规划与实施包括企业信息系统的基础数据、应用系统与业务的灾难备份与恢复计划。

3. 灾难恢复与灾难备份

灾难备份(Backup for Disaster Recovery)指为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份的过程。

灾难恢复(Disaster Recovery)指为了将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态而设

计的活动和流程。

4. 灾难恢复规划与灾难恢复预案

灾难恢复规划(Disaster Recovery Planning)指为了减少灾难带来的损失和保证信息系统所支持的关键业务功能在灾难发生后能及时恢复和继续运作所做的事前计划和安排。

灾难恢复预案(Disaster Recovery Plan)指定义信息系统灾难恢复过程中所需的任务、行动、数据和资源的文件。用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能。

5. BCP 和 BCM

业务连续规划(Business Continuity Planning,BCP)是灾难事件的预防和反应机制,是一系列事先制定的策略和规划,确保单位在面临突发的灾难事件时,关键业务功能能持续运作、有效地发挥作用,以保证业务的正常和连续。业务连续规划不仅仅包括对信息系统的恢复,而且包括关键业务运作、人员及其他重要资源等的恢复和持续。

业务连续性管理(Business Continuity Management,BCM)主要分为危机管理、应急管理和业务连续规划三部分。危机管理包括关联组织危机管理和危机通信及危机公关;应急管理包括紧急事件应急响应处置和灾难事件应急响应处置;业务连续规划包括风险分析和业务影响分析、恢复策略和方案、信息系统恢复预案、业务恢复预案及重建和回退计划,如图 4.7 所示。

业务连续管理(BCM)								
危机管理		应急管理		业务连续规划(BCP)				
关联组织危机管理	危机通信及危机公关	紧急事件应急响应处置	灾难事件应急响应处置	风险分析和业务影响分析	恢复策略和方案	信息系统恢复预案	业务恢复预案	重建和回退计划

图 4.7　业务连续管理

对于信息化依赖程度高的单位,信息系统灾难恢复是其业务连续规划的重要组成部分。信息系统灾难恢复的目的是保证信息系统所支持业务的连续,业务连续规划面向信息系统及业务恢复。

6. BCP/DRP 的指标——恢复点目标(RPO)和恢复时间目标(RTO)

恢复点目标 RPO(Recovery Point Objective)指灾难发生后,系统和数据必须恢复到的时间点要求。代表了当灾难发生时允许丢失的数据量。

恢复时间目标 RTO(Recovery Time Objective)指灾难发生后,信息系统或业务功能从停顿到必须恢复的时间要求。代表了系统恢复的时间。

7. 主中心与灾难备份中心

主中心也称主站点或生产中心,是指主系统所在的数据中心。

灾难备份中心也称备用站点,是指用于灾难发生后接替主系统进行数据处理和支持关键业务功能运作的场所,可提供灾难备份系统、备用的基础设施和专业技术支持及运行维护管理能力,此场所内或周边可提供备用的生活设施。

8. 主系统与灾难备份系统

主系统也称生产系统,是指正常情况下支持组织日常运作的信息系统,包括主数据、主数据处理系统和主网络。

灾难备份系统,是指用于灾难恢复目的,由数据备份系统、备用数据处理系统和备用的

网络系统组成的信息系统。

9. 灾难恢复建设流程

灾难恢复建设流程分为5个步骤。

（1）分析评估。该阶段主要进行目标和需求分析、风险分析和业务影响分析，是灾难恢复建设的启动阶段。

（2）架构设计。该阶段进行策略制订和方案预设，确定灾难恢复建设的执行策略和方案，是灾难恢复建设的计划阶段。

（3）开发实施。该阶段实行预案开发和制度制订，主要为BCP制订和方案实施，是灾难恢复建设的执行阶段。

（4）启动管理。该阶段包括演练和测评两部分内容，是灾难恢复建设的控制阶段。

（5）持续维护。该阶段分为日常维护和培训，主要工作是维护、审核和更新，是灾难恢复建设的结束阶段。

4.3.2 我国灾难恢复工作的进展情况和政策要求

1. 我国灾难恢复工作的进展情况

20世纪90年代末期，一些单位在信息化建设的同时，开始关注对数据安全的保护，进行数据的备份，但当时，不论从灾难恢复理论水平、重视程度、从业人员数量质量，还是技术水平方面都还很不成熟。2000年，“千年虫”事件引发了国内对于信息系统灾难的第一次集体性关注，但“9.11”事件所引起的震动真正地引起了大家对灾难恢复的关注。各行业用户对信息安全的建设越来越重视，投入呈现稳定增长的态势，但大部分单位还没有有效的灾难恢复策略，没有建立统一的业务连续管理机制。随着国内信息化建设的不断完善、数据大集中的开展和国家对灾难恢复工作的高度重视，越来越多的单位和部门认识到灾难恢复的重要性和必要性，开展灾难恢复建设的时机已基本成熟。

2. 我国灾难恢复工作的国家政策和标准

2003年，《国家信息化领导小组关于加强信息安全保障工作的意见》要求：各基础信息网络和重要信息系统建设要充分考虑抗毁性与灾难恢复，制定和不断完善信息安全应急处置预案。2004年，国信办《关于做好重要信息系统灾难备份工作的通知》强调了“统筹规划、资源共享、平战结合”的灾难备份工作原则。2005年，国务院信息化办公室发布《重要信息系统灾难恢复指南》；2007年，发布《信息安全技术信息系统灾难恢复规范》(GB/T 20988—2007)。

3. 我国灾难恢复地方和行业的发展

北京市、上海市、深圳市、广州市、成都市等地都已出台或正在研究电子政务信息系统灾难恢复工作的意见和规划；人民银行、银监会、保监会出台了有关行业政策；国税总局、海关总署、人民银行、商务部等部委均已完成或正在建设灾难备份中心；北京、上海、深圳、广州、杭州等各地政府已建设或启动灾难备份中心建设。其他信息化程度较高的行业如保险、证券、电力、民航、电信、石化、钢铁等企业正在开展和规划灾难恢复系统的建设。

4. 我国灾难恢复工作存在的主要问题

在我国灾难恢复工作中，主要存在以下问题：

（1）存在侥幸心理，缺乏开展灾难恢复工作的积极性。

(2) 在没有统筹规划，各行业及地方自行建设灾难备份中心，造成社会经济资源的分散和浪费。

(3) 从事灾难恢复建设和服务的企业良莠不齐，部分企业缺乏专业化能力，不能满足灾难恢复的要求。

(4) 已建成的灾难备份中心普遍缺乏严格的演练，灾难备份中心的运营缺乏有效的监管和审计，导致大量的灾难备份中心无法在灾难来临时有效发挥作用。

(5) 灾难备份恢复有关人员意识欠缺、专业人才缺乏。

4.3.3 数据储存和数据备份与恢复的基本技术

1. 需要备份的数据类型

系统数据主要是指操作系统、数据库系统安装的各类软件包和应用系统执行程序。系统数据在系统安装后基本上不再变动，只有在操作系统、数据库系统版本升级或应用程序调整时才发生变化。系统数据一般都有标准的安装介质，如软盘、磁带、光盘。

基础数据主要是指保证业务系统正常运行所使用的系统资产清单、用户清单、系统配置文件、网络配置文件、应用配置文件、存取权限控制等。基础数据随业务系统运行环境的变化而变化，一般作为系统档案进行保存。

应用数据主要是指业务系统的所有业务数据，对数据的安全性、准确性、完整性、一致性要求很高，而且变化频繁。

临时数据主要是指操作系统、数据库产生的系统运行记录、数据库逻辑日志和应用程序在执行过程中产生的各种打印、传输临时文件，随系统运行和业务的发生而变化。

备份类型分为全备份、增量备份和差分备份 3 种类型。

(1) 全备份。对整个系统所有文件进行完全备份，包括所有系统和数据。

(2) 增量备份。每次备份的数据只是相当于上一次备份后增加和修改过的数据。

(3) 差分备份。每次备份的数据是相对于上一次全备份之后新增加和修改过的数据。

2. 数据存储技术

数据存储技术有直接附加存储(DAS)、网络附加存储(NAS)和存储区域网络(SAN)，现对 3 种技术做详细解释。

(1) DAS，通过电缆(SCSI)或光缆(FC)将存储设备直接连接到服务器上。它能适应服务器地理分布分散的情况；实现大容量存储；实现操作系统与数据的分离；提高存取性能；实施简单。但是，它对服务器依赖性强，占用服务器资源；可扩展性差，扩展时需要停机；资源利用率低；可管理性差；异构化严重。

(2) NAS，不再通过 I/O 总线附属于某个特定的服务器，而是通过网络接口将存储设备与网络相连，由用户通过网络访问，由存储设备、NAS 控制器和网络部分构成。目前采用 NFS(基于 UNIX 环境的网络文件系统)和 CIFS(基于 Windows 的网络文件系统)协议。它具有以下优点：一台设备连接在网络上，易于安装、部署和管理；不占用服务器资源；可以跨平台使用；较 DAS 节省硬盘空间；数据集中，便于管理和备份。但是，它占用网络带宽；不易扩展，装一台 NAS 设备容易，再加一台难。

(3) SAN，通过网络设备将磁盘阵列等存储设备与服务器连接起来的高速专用子网。根据专用网络的不同可以分为 FC-SAN 和 IP-SAN。它的数据存储影响服务器和网络的性

能;效率高、容量大、可扩展性强;支持异构服务器。但是,它价格高,对小型系统不划算;服务器物理位置很分散时不易实施。

3. 数据复制模式和常见的形式

数据复制的模式：同步(Synchronous),数据高可用、对性能影响大、有距离限制;异步(Asynchronous),数据有延迟、适于远距离;定点复制(Point-in-time),数据有延迟、适于远距离、充分利用网络带宽。数据复制的常见形式有以下几种：

(1) 基于主机的数据复制(操作系统的 I/O 完成)。与存储设备无关、数据完全一致、灵活、对带宽要求高、对不同的操作系统需要专用的软件、需要管理多个节点、需占用主机的处理能力。

(2) 基于数据库的数据复制(操作系统和数据库系统共同完成)。灵活、方便、对带宽要求低、通过复制数据库重做日志来复制数据库数据、适用范围窄。

(3) 基于磁盘的数据复制(存储系统的微处理器完成)。与主机无关、可支持异构平台环境、带宽要求高、主备端需要使用同样的磁盘存储系统、在远程情况下需要配置专用的通道延伸器、成本较高。

(4) 基于专有设备的数据复制(在 SAN 架构中通过虚拟存储软件完成)。在数据从服务器传输到存储设备的网络中抓取数据。任意的存储设备之间进行复制、通过异步机制对数据的定点副本(point-in-time images)进行复制,确保数据的一致性,可点对点或多点对一点进行复制。

4. 负载均衡

负载均衡 (Load Balancing) 建立在现有网络结构之上,它提供了一种廉价、有效、透明的方法扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性。负载均衡(又称为负载分担),英文名称为 Load Balance,其意思就是将负载(工作任务)进行平衡、分摊到多个操作单元上执行,如 Web 服务器、FTP 服务器、企业关键应用服务器和其他关键任务服务器等,从而共同完成工作任务。通过负载均衡(Load Balance)、流量(Traffic)可以被动态(Dynamically)分配到一组运行相同应用程序的多个服务器上。负载均衡既可以提高整个系统的性能,又可以在服务器出现故障时将该服务器承担的服务分配到运行中的服务器执行。在不同站点的服务器之间进行的负载均衡还可以在某一站点无法提供服务时将该站点承担的服务分配到运行中的站点执行。

4.3.4 灾难恢复管理过程

1. 灾难恢复需求分析

风险评估对为什么需要灾难恢复建设这一问题给出了以下答案。

做好风险分析,以便能够为机构提供以下服务：

(1) 辨认足以影响机构持续提供业务的各种潜在性风险。

(2) 确定各种风险发生的可能性。

(3) 制定并实施各特定风险的预防控制措施,为残余风险的应对处理做好准备。

风险分析的范围是机构所在地区范围和与之在经济、业务上有紧密联系的邻近地区的交通、电信、能源及其他关键基础设施遭到严重破坏的风险;造成此地区的大规模人口疏散或无法联系后所面对的风险;机构信息系统中断所造成的系统性风险。

BIA(业务影响分析):明确关键业务功能和支持关键业务功能的关键应用系统;明确系统中断对业务的损失和影响;明确各业务系统的恢复目标和内外部依赖关系;确定各业务功能灾难恢复指标(RTO/RPO);明确各业务功能恢复的最小资源需求及恢复策略。

确定灾难恢复目标。根据风险分析和业务影响分析的结果,确定灾难恢复目标,包括:关键业务功能及恢复的优先顺序;灾难恢复时间范围,即 RTO 和 RPO 的范围。

2. 制定灾难恢复策略

灾难恢复策略是机构为了达到灾难恢复的需求目标而采取的途径,它包含实现的计划、方法和可选的方案,是基于机构对自身灾难恢复需求确切了解的基础上做出的;其根本目的是为了达到在灾难恢复需求中描述的实现目标,是指导整个灾难恢复建设的纲领性文件。要遵循成本风险平衡原则;描述了灾难恢复需求的实现步骤和实现方法。

3. 灾难恢复的实现

1) 灾难备份中心的选择和建设

灾难备份中心的选址原则如图 4.8 所示。

策略性
明确对灾难备份中心的定位,即灾难备份中心的建设目的是防范什么样的灾难事件,在灾难发生的时候又能够提供何种服务
风险性
选择或建设灾难备份中心时,要注意备选的场址所包含的风险是否是在单位所容忍的风险范围之内,或者是符合所制定灾难恢复规划或业务连续性管理的要求
科学性
选择或建设灾难备份中心时,应对备选的场址进行相关的场地风险分析,科学、全面地评价各备选的场址
适合性
基础设施符合《电子计算机场地通用规范》(GB/T 2887—2000)的要求。关注场址周边环境、地质地理条件、市政配套条件、电力供应条件、通信服务商所能提供的服务能力等诸多因素
便捷性
对于灾难备份中心,其周边应有多条道路用于保证相关人员和物资能顺利、快速到达
选址原则

图 4.8 选址原则

灾难备份中心的基础设施分为 3 种类型:第一种为工作设施,分为信息系统工作设施和保障系统工作设施;第二种为辅助设施,分为灾难备份中心辅助设施、灾难恢复辅助设施和灾难恢复培训设施;第三种为生活设施,分为保障人员生活设施和灾难恢复人员生活设施,如表 4.1 所示。

表 4.1 基础设施要求

设施类型	设施名称	说　明
工作设施	信息系统工作设施	位于灾难备份中心的核心区域的信息系统设备及相关配套设备,主要包括计算机机房、主操作室、通信机房、介质机房、信息系统设备测试维修机房等
	保障系统工作设施	位于灾难备份中心的保障设备区域,用来保障灾难备份中心 7×24h 运行的设施,主要包括供配电设施、空调暖通设施、给排水设施、消防设施、监控设施、货运设施等

续表

设施类型	设施名称	说　　明
辅助设施	灾难备份中心辅助设施	用于灾难备份中心运行所需的配套设施，主要包括灾难备份中心办公室、会议室、资料室、值班室、仓库、客户接待室、客户休息室、客户活动区域、停车场、货物装卸区等
	灾难恢复辅助设施	灾难备份中心中提供灾难恢复用途的设施，主要包括灾难恢复指挥中心、灾难恢复座席区、办公区、新闻发布中心(多媒体室)、会议室、打印传真室等
	灾难恢复培训设施	灾难备份中心中提供用于灾难恢复或业务连续性培训的设施，主要包括培训教室、模拟演练室、培训人员办公室等
生活设施	保障人员生活设施	提供给灾难备份中心 7×24h 运行而配备的人员生活所必需的设施，主要包括宿舍、食堂、健身房、阅览室等生活设施
	灾难恢复人员生活设施	提供给灾难恢复或灾难恢复培训人员所需要的生活设施，主要包括客房、食堂等生活设施

2）灾难备份系统技术方案的实现

根据灾难恢复策略制定相应的灾难备份系统技术方案，包含数据备份系统、备用数据处理系统和备用的网络系统。技术方案中所设计的系统，应获得同主系统相当的安全保护；具有可扩展性；考虑其对主系统可用性和性能的影响。为确保技术方案满足灾难恢复策略的要求，应由组织的相关部门对技术方案进行确认和验证，并记录和保存验证及确认的结果。按照确认的灾难备份系统技术方案进行开发，实现所要求的数据备份系统、备用数据处理系统和备用网络系统。按照经过确认的技术方案，灾难恢复规划实施组织应制定各阶段的系统安装及测试计划，以及支持不同关键业务功能的系统安装及测试计划，并组织最终用户共同进行测试。确认以下各项功能可以正确实现：数据备份及数据恢复功能；在限定的时间内，利用备份数据正确恢复系统、应用软件及各类数据，并可正确恢复各项关键业务功能；客户端可与备用数据处理系统通信正常。

3）技术支持能力的实现

组织应根据灾难恢复策略的要求，获取对灾难备份系统的专业技术支持能力。灾难备份中心应建立相应的技术支持组织，定期对技术支持人员进行技能培训。

4）运行维护管理能力的实现

为了达到灾难恢复目标，灾难备份中心应建立各种操作规程和管理制度，用以保证以下各方面的实现：数据备份的及时性和有效性；备用数据处理系统和备用网络系统处于正常状态，并与主系统的参数保持一致；有效的应急响应、处理能力。

5）灾难恢复预案的实现

灾难恢复的每个等级均应按具体要求制定相应的灾难恢复预案，并进行落实和管理。

6）灾难恢复预案的制定、落实和管理

灾难恢复预案包括的主要内容为：确定风险场景；描述可能受到的业务影响；描述使用的预防性策略；描述灾难恢复策略；识别和排列关键应用系统；行动计划；团队和人员的职责；联络清单；所需资源配置等。制定灾难恢复预案的原则：首先，必须集中管理灾难恢复预案的版本和发布；其次，为了建立有效的版本控制体系，必须建立规范的灾难恢复预案的问题提交、解决、更新、跟踪、发布的渠道和流程；第三，建立相关的保密管理规定，保证灾难恢复预案中涉及的秘密信息得到保护；第四，灾难恢复预案在内容管理方面应注意内容的分

布和粒度，可根据版本和内容的更新频度将灾难恢复的内容进行适当的分布；第五，建立合理的灾难恢复预案的保管制度，强调存放的安全性和易取得性。

成功预案的特点：清楚、简洁；高级管理层支持/组织承诺；不断改进和更新的恢复策略；及时的更新维护；组织职责分工明确；保留、备份和异地存储计划；完整记录并定期演练；风险得到管理；弱点得到优先重视；灵活、可适应。

在灾难来临前使相关人员了解、熟悉恢复流程，使灾难恢复预案得到理解并可以使用，促进灾难恢复预案活动、更新、实用；展示恢复的能力，达到法律和内部审计要求。

演练和演习的主要方式有桌面演练、模拟演练、实战演练等。根据演练和演习的深度，可分为系统级演练、应用级演练、业务级演练等。根据演练和演习的准备情况，可分为计划内的演练和演习、计划外的演练和演习等。

预案恢复的管理包括维护管理和变更管理。维护管理包括：核对预案的功能性；验证预案文档的精确性和完整性；分发更新的文档：文档计划分发和发布流程；确保相关的团队收到更新的文档；依靠维护来改变管理流程；提供培训作为持续维护预案的一部分：为与灾难恢复的相关人员开展定期培训，如复习进修课程或灾难备份研讨会；指派培训责任，如部门经理要确保员工被送去参加培训；完成时报告预案维护情况；毁掉旧灾难恢复预案的复印件或电子版本。

变更管理是指对业务操作的增长或变化进行的管理，如：新的分支、产品和业务功能的增加；公司所有权的变化；关键人员的变化；硬件配置的变化；使用新操作系统；预案审核和演练后；软件/应用软件的变化；新的法律或审计要求；定期审核和更新，如每年两次。

7）灾难恢复资源要素与等级

灾难恢复包括七大技术管理要素和6个灾难恢复等级。根据国家标准《信息安全技术 信息系统灾难恢复规范》(GB/T 20988)，将灾难恢复划分为6个等级。6个等级由低到高分别为基本支持、备用场地支持、电子传输和部分设备支持、电子传输和完整设备支持、实时数据传输及完整设备支持以及数据零丢失和远程集群支持，如图4.9所示。

等级七要素
第1级 基本支持
第2级 备用场地支持
第3级 电子传输和部分设备支持
第4级 电子传输和完整设备支持
第5级 实时数据传输及完整设备支持
第6级 数据零丢失和远程集群支持
数据备份系统
备用数据处理系统
备用网络系统
备用基础设施
技术支持能力
运行维护支持
灾难恢复预案
最高 最低

图4.9 灾难恢复等级划分

根据国家标准《信息安全技术信息系统灾难恢复规范》(GB/T 20988),将灾难恢复划分为 7 个要素。7 个要素分别为数据备份系统、备用数据处理系统、备用网络系统、备用基础设施、技术支持能力、运行维护支持、灾难恢复预案,描述如表 4.2 所示。

表 4.2 灾难恢复资源要素

灾难恢复要素	描　　述
数据备份系统	一般由数据备份的硬件、软件和数据备份介质(以下简称"介质")组成,如果是依靠电子传输的数据备份系统,还包括数据备份线路和相应的通信设备
备用数据处理系统	指备用的计算机、外围设备和软件
备用网络系统	最终用户用来访问备用数据处理系统的网络,包含备用网络通信设备和备用数据通信线路
备用基础设施	灾难恢复所需的、支持灾难备份系统运行的建筑、设备和组织,包括介质的场外存放场所、备用的机房及灾难恢复工作辅助设施,以及容许灾难恢复人员连续停留的生活设施
技术支持能力	对灾难恢复系统的运转提供支撑和综合保障的能力,以实现灾难恢复系统的预期目标。包括硬件、系统软件和应用软件的问题分析和处理能力、网络系统安全运行管理能力、沟通协调能力等
运行维护支持	包括运行环境管理、系统管理、安全管理和变更管理等
灾难恢复预案	定义信息系统灾难恢复过程中所需的任务、行动、数据和资源的文件。用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能

4.3.5 国家有关标准对灾难恢复系统级别和各级别的指标要求

1. 第一级——基本支持

灾难恢复等级的第一级为基本支持。对该级别的指标要求应满足国标《信息系统灾难恢复规范》(GB/T 20988—2007)灾难恢复等级第 1 级要求:完全数据备份至少每周一次;备份介质场外存放;有介质存取、验证和转储管理制度;按介质特性对备份数据进行定期的有效性验证;在灾难恢复时,可享有规范运行的数据中心环境和 7×24h 专业技术支持,如表 4.3 所示。

表 4.3 第 1 级灾难恢复的指标要求

要　　素	要　　求
数据备份系统	① 完全数据备份至少每周一次 ② 备份介质场外存放
备用数据处理系统	—
备用网络系统	—
备用基础设施	有符合介质存放条件的场地
技术支持能力	—
运行维护支持	① 有介质存取、验证和转储管理制度 ② 按介质特性对备份数据进行定期的有效性验证
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

2. 第二级——备用场地支持

灾难恢复等级的第二级为备用场地支持。对该级别的指标要求应满足国标《信息系统灾难恢复规范》(GB/T 20988—2007)灾难恢复等级第2级要求：可为客户的媒体数据提供保护；客户节省了对机房建设及机房配套设施的大量投资和长时间的建设周期，直接获得了符合国家标准的机房环境和严格规范的机房管理服务；提供必要的网络接入端口，大大减少客户临时申请线路的长时间周期；用户可尽快完成有关设备系统的置备和安装，迅速恢复业务；在灾难恢复时，可享有规范运行的数据中心环境和7×24h专业技术支持，如表4.4所示。

表4.4　第2级灾难恢复的指标要求

要　素	要　　求
数据备份系统	① 完全数据备份至少每周一次 ② 备份介质场外存放
备用数据处理系统	灾难发生时能在预定时间内调配所需的数据处理设备到场
备用网络系统	灾难发生时能在预定时间内调配所需的通信线路和网络设备到位
备用基础设施	① 有符合介质存放条件的场地 ② 有满足信息系统和关键业务功能恢复运作要求的场地
技术支持能力	—
运行维护支持	① 有介质存取、验证和转储管理制度 ② 按介质特性对备份数据进行定期的有效性验证 ③ 有备用站点管理制度 ④ 与相关厂商有符合灾难恢复时间要求的紧急供货协议 ⑤ 与相关运营商有符合灾难恢复时间要求的备用通信线路协议
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

3. 第三级——电子传输和部分设备支持

灾难恢复等级的第三级为电子传输和部分设备支持。对该级别的指标要求应满足国标《信息系统灾难恢复规范》(GB/T 20988—2007)灾难恢复等级第3级要求：可为客户的媒体数据提供保护；可以使客户在24～48h内恢复业务的运作；节省客户在备份机房建设和备份主机设备等方面的大量投资；提供备份网络接入设备和网络接口，可以帮助客户迅速恢复服务渠道和分支机构的业务运作；在灾难恢复时，可享有规范运行的数据中心环境和7×24h专业技术支持，如表4.5所示。

表4.5　第3级灾难恢复的指标要求

要　　素	要　　求
数据备份系统	① 完全数据备份至少每天一次 ② 备份介质场外存放 ③ 每天多次利用通信网络将关键数据定时批量传送至备用场地
备用数据处理系统	配备灾难恢复所需的部分数据处理设备
备用网络系统	配备部分通信线路和相应的网络设备

续表

要　　素	要　　求
备用基础设施	① 有符合介质存放条件的场地 ② 有满足信息系统和关键业务功能恢复运作要求的场地
技术支持能力	在备用站点有专职的计算机机房运行管理人员
运行维护支持	① 有介质存取、验证和转储管理制度 ② 按介质特性对备份数据进行定期的有效性验证 ③ 有备用计算机机房管理制度 ④ 有备用数据处理设备硬件维护管理制度 ⑤ 有电子传输数据备份系统运行管理制度
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

4. 第四级——电子传输和完整设备支持

灾难恢复等级的第四级为电子传输和完整设备支持。对该级别的指标要求应满足国标《信息系统灾难恢复规范》(GB/T 20988—2007)灾难恢复等级第 4 级要求：节省客户在备份机房建设和备份主机设备等方面的大量投资；享有 7×24h 备份中心的专业技术支持和专业规范长期运营队伍支持；客户数据得到在线电子传输方式的备份，可使客户数据的丢失范围控制在 24h 之内；在备份中心为客户建立了备份的主机系统及网络系统，并有快速恢复措施，业务恢复时间可控制在 8～24h 之内，如表 4.6 所示。

表 4.6　第 4 级灾难恢复的指标要求

要　　素	要　　求
数据备份系统	① 完全数据备份至少每天一次 ② 备份介质场外存放 ③ 每天多次利用通信网络将关键数据定时批量传送至备用场地
备用数据处理系统	配备灾难恢复所需的全部数据处理设备，并处于就绪状态或运行状态
备用网络系统	① 配备灾难恢复所需的通信线路 ② 配备灾难恢复所需的网络设备，并处于就绪状态
备用基础设施	① 有符合介质存放条件的场地 ② 有符合备用数据处理系统和备用网络设备运行要求的场地 ③ 有满足关键业务功能恢复运作要求的场地 ④ 以上场地应保持 7×24h 运作
技术支持能力	在备用站点有： ① 7×24h 专职计算机机房管理人员 ② 专职数据备份技术支持人员 ③ 专职硬件、网络技术支持人员
运行维护支持	① 有介质存取、验证和转储管理制度 ② 按介质特性对备份数据进行定期的有效性验证 ③ 有备用计算机机房运行管理制度 ④ 有硬件和网络运行管理制度 ⑤ 有电子传输数据备份系统运行管理制度
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

5. 第五级——实时数据传输与完整设备支持

灾难恢复等级的第五级为实时数据传输与完整设备支持。对该级别的指标要求应满足国标《信息系统灾难恢复规范》(GB/T 20988—2007)灾难恢复等级第5级要求:节省客户在备份机房建设和备份主机设备等方面的大量投资;享有7×24h备份中心的专业技术支持和专业规范长期运营队伍支持;客户数据得到在线实时传输备份,可使客户数据的丢失范围控制在秒级到几小时之内;备份中心主机与备份网络均实时运行和处于随时就绪状态,业务恢复时间可控制在宣告灾难后几十分钟至几小时之内,如表4.7所示。

表4.7 第5级灾难恢复的指标要求

要　　素	要　　求
数据备份系统	① 完全数据备份至少每天一次 ② 备份介质场外存放 ③ 采用远程数据复制技术,并利用通信网络将关键数据实时复制到备份场地
备用数据处理系统	配备灾难恢复所需的全部数据处理设备,并处于就绪或运行状态
备用网络系统	① 配备灾难恢复所需的通信线路 ② 配备灾难恢复所需的网络设备,并处于就绪状态 ③ 具备通信网络自动或集中切换能力
备用基础设施	① 有符合介质存放条件的场地 ② 有符合备用数据处理系统和备用网络设备运行要求的场地 ③ 有满足关键业务功能恢复运作要求的场地 ④ 以上场地应保持7×24h运作
技术支持能力	在备用站点7×24h有专职的: ① 计算机机房管理人员 ② 数据备份技术支持人员 ③ 硬件、网络技术支持人员
运行维护支持	① 有介质存取、验证和转储管理制度 ② 按介质特性对备份数据进行定期的有效性验证 ③ 有备用计算机机房运行管理制度 ④ 有硬件和网络运行管理制度 ⑤ 有实时数据备份系统运行管理制度
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

6. 第六级——数据零丢失和远程集群支持

灾难恢复等级的第六级为零数据丢失和远程集群支持。对该级别的指标要求应满足国标《信息系统灾难恢复规范》(GB/T 20988—2007)灾难恢复等级第6级要求:节省客户在备份机房建设等方面的大量投资;享有7×24h备份中心的专业技术支持和专业规范长期运营队伍支持;客户数据得到实时同步更新,保证业务数据的一致性和完整性;备份中心的远程集群系统及网络系统可自动进行负载均衡和系统切换,业务恢复时间可控制在分钟级,如表4.8所示。

表 4.8　第 6 级灾难恢复的指标要求

要　　素	要　　求
数据备份系统	① 完全数据备份至少每天一次 ② 备份介质场外存放 ③ 远程实时备份，实现数据零丢失
备用数据处理系统	① 备用数据处理系统具备与生产数据处理系统一致的处理能力并完全兼容 ② 应用软件是“集群的”，可实时无缝切换 ③ 具备远程集群系统的实时监控和自动切换能力
备用网络系统	① 配备与生产系统相同等级的通信线路和网络设备 ② 备用网络处于运行状态 ③ 最终用户可通过网络同时接入主、备中心
备用基础设施	① 有符合介质存放条件的场地 ② 有符合备用数据处理系统和备用网络设备运行要求的场地 ③ 有满足关键业务功能恢复运作要求的场地 ④ 以上场地应保持 7×24h 运作
技术支持能力	在备用站点 7×24h 有专职的： ① 计算机机房管理人员 ② 专职数据备份技术支持人员 ③ 专职硬件、网络技术支持人员 ④ 专职操作系统、数据库和应用软件技术支持人员
运行维护支持	① 有介质存取、验证和转储管理制度 ② 按介质特性对备份数据进行定期的有效性验证 ③ 有备用计算机机房运行管理制度 ④ 有硬件和网络运行管理制度 ⑤ 有实时数据备份系统运行管理制度 ⑥ 有操作系统、数据库和应用软件运行管理制度
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

4.4　本章小结

系统获取开发和维护部分，介绍了系统的获取、开发和维护。系统的获取应该符合系统获取的原则，获取系统的方法：可以从外部购买，购买时依照系统购买流程购买系统，并注意购买过程中的安全问题；也可以自己开发，开发应遵循系统开发流程，注意开发过程中的安全问题。系统在使用时应该注意维护，系统维护部分介绍了维护的内容和类型、变更管理、紧急变更及补丁和漏洞管理的知识。

信息安全事件管理与应急响应部分，详细介绍了信息安全事件管理与应急响应的基本概念，同时介绍了我国信息安全事件管理与应急响应工作的进展情况和政策要求，信息安全应急响应阶段方法论、信息安全应急响应计划编制方法和应急响应小组的作用和建立方法应该重点掌握，理解各个应急小组的职能，了解我国信息安全事件分级分类方法及国际和我国信息安全应急响应组织。现在，打击信息技术犯罪的一项有效手段是计

算机取证技术，介绍了计算机取证的概念和作用以及计算机取证的原则、基本步骤、常用方法和工具。

业务连续性管理与灾难恢复部分，详细介绍了业务连续性管理与灾难恢复的基本概念，我国灾难恢复工作的进展情况和政策要求，数据储存和数据备份与恢复的基本技术的相关概念和知识，灾难恢复管理过程，同时详细介绍了灾难恢复系统的 6 个级别和 7 个要素，以及各级别的指标要求，这个知识点应该重点掌握。

第 5 章　信息安全管理华为典型实例

导入语：本章系统地介绍了华为内网安全的解决方案、终端安全管理解决方案和 H3C 终端接入控制解决方案。

本章主要知识结构如图 5.1 所示。

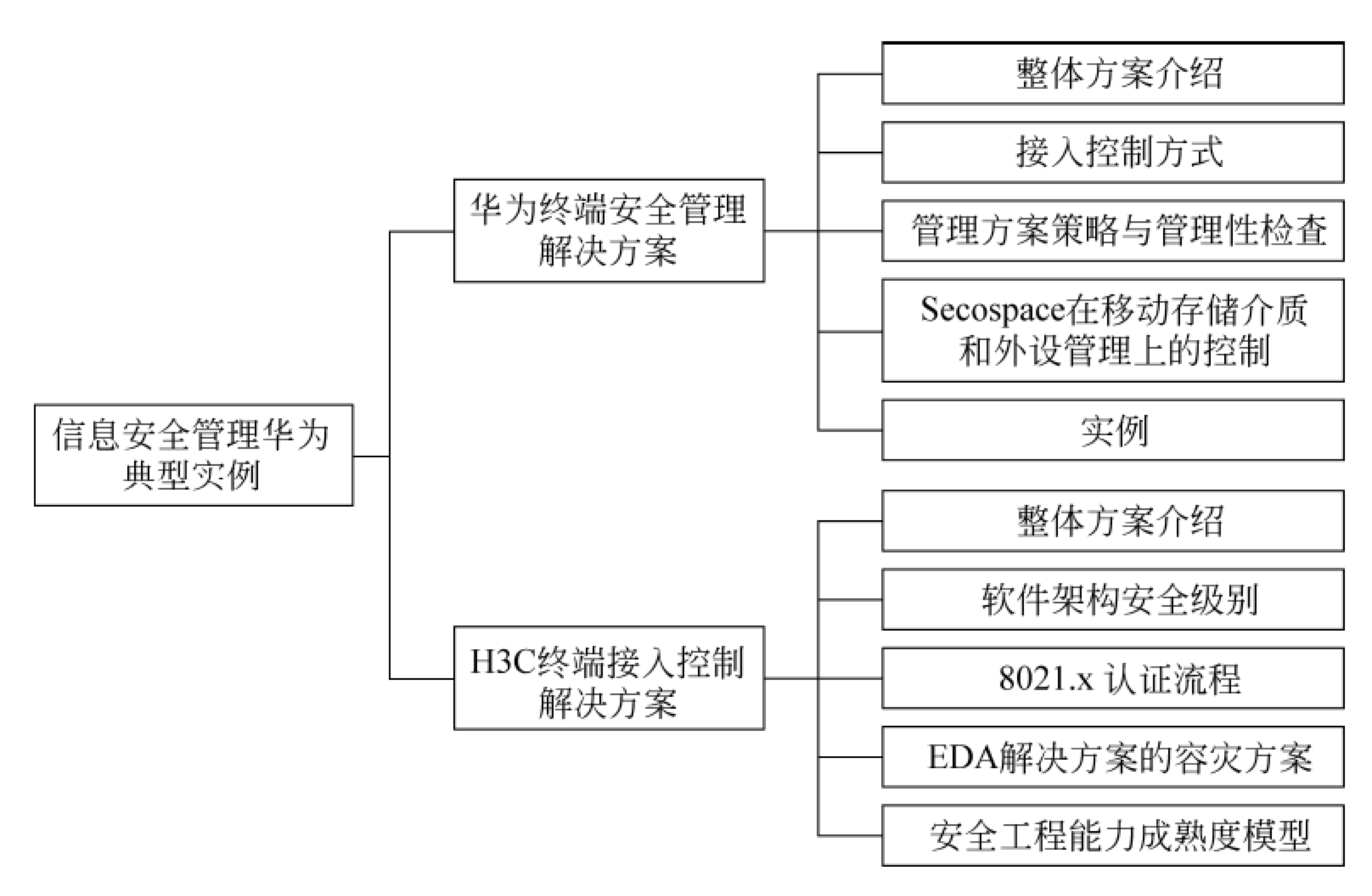


图 5.1　本章主要知识结构框图

在创新无处不在的 IT 世界里，从要求可用性到安全性再到高效率，只经历了短短的几年时间。而在 IT 管理概念中，时至今日终端管理无疑已经成为最重要的内容之一，它同样遵循着从可用性到安全性再到追求效率的发展规律。萨班斯-奥克斯利法案(Sarbanes-Oxley Act of 2002)对维护网络信息的安全性、保密性和完整性就提出了相关要求，而要达到这些要求，对终端的有效管理是解决问题的根本之道。是否能有一套完整的管理方案可同时解决终端的可用性、安全性和高效率呢？为了解决这个问题，H3C 推出了 H3C EAD (H3C End user Admission Domination)终端准入控制解决方案。H3C EAD 解决方案伴随着 IT 管理的发展，从最早实现用户身份认证，到实现网络安全认证，再到实现终端高效管理，也完成了从保障网络的可用性到安全性再到高效率的变化。H3C EAD 解决方案截至 2008 年 5 月，在现网中使用的用户数已经突破 40 万，这个变化不仅是一个数字的变化，更是代表了业界终端管理水平在质的方面的飞跃。

考核目标：熟悉并掌握华为的内网安全解决方案，终端安全管理解决方案和 H3C 终端接入控制解决方案。

5.1　内网安全危机

互联网的迅速普及，网络应用已成为企业发展中必不可少的一部分。然而，企业在感受网络所带来便利的同时，也面临着各种各样的进攻和威胁，如机密泄露、数据丢失、网络滥

用、身份冒用、非法入侵等。目前有些企业建立了相应的网络安全系统，并制定了相应的网络安全使用制度。但在实际使用中，由于用户对操作系统安全使用策略的配置及各种技术选项意义不明确，各种安全工具得不到正确的使用，系统漏洞、违规软件、病毒、恶意代码入侵等现象层出不穷，导致用户计算机操作系统达不到等级标准要求的安全等级。

5.1.1 内网安全危机

在今天的信息时代，基于网络的威胁潜伏在企业的每一个角落。随着企业和组织网络规模的增大，分支机构、移动办公、访客等增加了网络中的接入点，使存在于各层的网络漏洞成倍增加，病毒泛滥、未及时安装补丁招致恶意攻击、员工及合作伙伴盗窃机密数据等问题，成为企业面临的首要安全威胁。

5.1.2 内部威胁为首的主要安全问题

据 ISCA 统计，全球每年仅仅由于信息安全问题导致的损失高达数百亿美元，其中来自于内部的威胁高达 60%，来自内部的威胁已经成为企业首要的安全问题。企业面临的威胁复杂多样，其中主要有以下 3 个方面：

(1) 企业内网面临复杂多样的威胁。

非法用户随意接入公司内部网络；内部合法用户滥用权限；员工私自安装软件、开启危险服务；员工私自访问与工作无关网站；员工绕过防火墙访问互联网；员工未安装防病毒软件；员工忘记设置必要的口令等。

(2) 现有安全设备难以有效保护网络。

无法检查网络内计算机的安全状况；缺乏对合法终端滥用网络资源的安全管理；无法防止恶意终端的蓄意破坏。

(3) 终端数量大系统复杂、员工行为难以管理。

企业内网缺乏有效安全监控、审计手段；系统缺乏行之有效的管理及紧急响应手段；无法跟踪恶意员工泄露企业信息；员工上网等行为难以审计与管理；无法及时掌握终端的更新和变化。

5.1.3 确保企业内网安全，解决安全威胁问题

为确保企业内网的安全，必须强化内防内控，从终端入手强化弱点管理，着力解决终端接入控制；终端访问授权；终端安全健康性检查与策略管理；员工行为管理与违规审计等安全威胁问题。

(1) 终端接入控制。防止非法终端的接入，降低不安全终端的威胁。

(2) 终端访问授权。防止合法终端越权访问，保护企业核心资源。

(3) 终端安全健康性检查与策略管理。帮助企业落实安全管理制度。

(4) 员工行为管理与违规审计。强化行为审计，防止恶意终端破坏。

5.2 华为终端安全管理解决方案分析

5.2.1 华为终端安全管理解决方案

1. 信息安全策略的目标

信息安全策略的目标是为信息安全提供管理指导和支持，并与业务要求和相关的法律

法规保持一致。本策略主要包含以下 4 个方面：

（1）策略下发。必须得到管理层批准，并向所有员工和相关第三方传达，全体人员必须履行相关的义务，享受相应的权利，承担相关的责任。

（2）策略维护。信息安全策略通过以下方式进行文档的维护工作：

必须每年按照《风险评估管理程序》进行例行的风险评估，如遇以下情况必须及时进行风险评估。例如，发生重大安全事故；组织或技术基础结构发生重大变更；安全管理小组认为应当进行风险评估的；其他应当进行安全风险评估的情形，风险评估之后根据需要进行安全策略条目修订，并公布传达。

（3）策略评审。每年必须参照《管理评审程序》执行公司管理评审。

（4）适用范围。信息管理策略使用和涵盖的对象，包括现有的业务系统、硬件资产、软件资产、信息、通用服务、物理安全区域等。

2. 华为终端安全管理的解决方案

华为终端安全管理解决方案采取未雨绸缪的方式在端点接入网络之前进行安全状态评估，并提供系统漏洞修复，从而将病毒屏蔽在网络之外，同时强制应用级的安全策略，持续监控用户网络行为，包括移动存储设备管理，并对重要数据进行主动加密和严格的访问权限控制，最后还提供必要的系统应用管理，包括软件分发和资产管理。

根据终端安全管理模型，该方案采用了包括定制策略—检查控制—修复加固—统计汇总—持续审计的整体解决思路。

该方案还通过一体化、多层次和全面内网安全管理，实现企业从被动响应到有预见性、主动性的防御方式转变。

3. 终端安全管理带来的价值

终端安全管理给管理带来的价值有以下 4 个方面。

（1）通过身份和安全双重认证、隔离、修复、授权、审计的接入控制模式，保障企业网络内部终端安全性，提高企业网络内部终端安全水平。

（2）丰富的可灵活配置的终端管理策略，将终端管理经验融入其中，帮助企业快速部署和实现适合自身的终端管理。

（3）强制安全检查，用户行为审计，确保企业管理制度的落实；实现细粒度的基于用户的访问控制，严格控制终端对业务系统的访问范围，保护业务系统的安全。

（4）灵活的部署，方便的管理，丰富的报表，友好的界面，在有效提高企业终端管理水平的同时降低企业维护成本。

4. Secospace 终端安全管理系统的组成部分

Secospace 终端安全管理系统由安全代理（SA）、安全管理器（SM）、安全控制器（SC）、安全准入控制网关（SACG）、TSM 管理中心（TMC）五部分组成。每部分功能如下。

SM 作为系统的核心管理服务器，管理多个 SC。SM 采用 B/S 架构，系统管理员可通过 Web 界面配置和修改用户信息、访问权限和策略等，并完成报表输出。

SC：SC 作为与 SA 交互的控制点，是系统管理功能的实施者。完成用户身份认证、安全策略下发和软件下发等任务。并与 802.1X 或 SACG 联动在完成身份认证和安全策略检查后，开放端口或匹配 ACL 规则授权用户访问网络资源。

SA：SA 安装于客户的 PC 上，向服务器获取安全策略参数，根据这些参数执行本地计算机的安全策略检查；实施监控终端的行为，并且把审计的结果上报服务器，作为审计的

证据。

SACG：SACG 是在华为电信级防火墙硬件平台上开发的专用的接入控制网关，是实现硬件网关接入控制方式的核心设备。

TMC：TSM 的快速恢复服务器和 TSM 快速恢复客户端可通过 TSM 管理中心以最快的速度进行托管。通过一个单一的用户界面，可以管理端到端的数据保护和恢复。TSM 服务器 hztsmserver1 默认是自动启动的，并且每次机器重启后都是自动启动的。自动功能是通过/etc/inittab 文件中的启动脚本来实现的。

据专业的网络安全评估专家建议，对网络内部终端和公共可访问的服务器到 Internet 或其他不可信网络的外出流量都应该进行过滤，以阻止黑客和蠕虫的“抓钩”攻击。SACG 对终端的所有上行流量进行过滤，将网络分为可信、非受信和 DMZ(Trusted、Untrusted 和 DMZ)3 个域，用户在没有通过身份认证和安全检查前只能访问 DMZ，即受限的认证前域。通过后才能基于用户角色开放相应可以访问的认证后域，提供有效的内网接入保护。安全接入控制网关 SACG 方式的拓扑结构如图 5.2 所示。

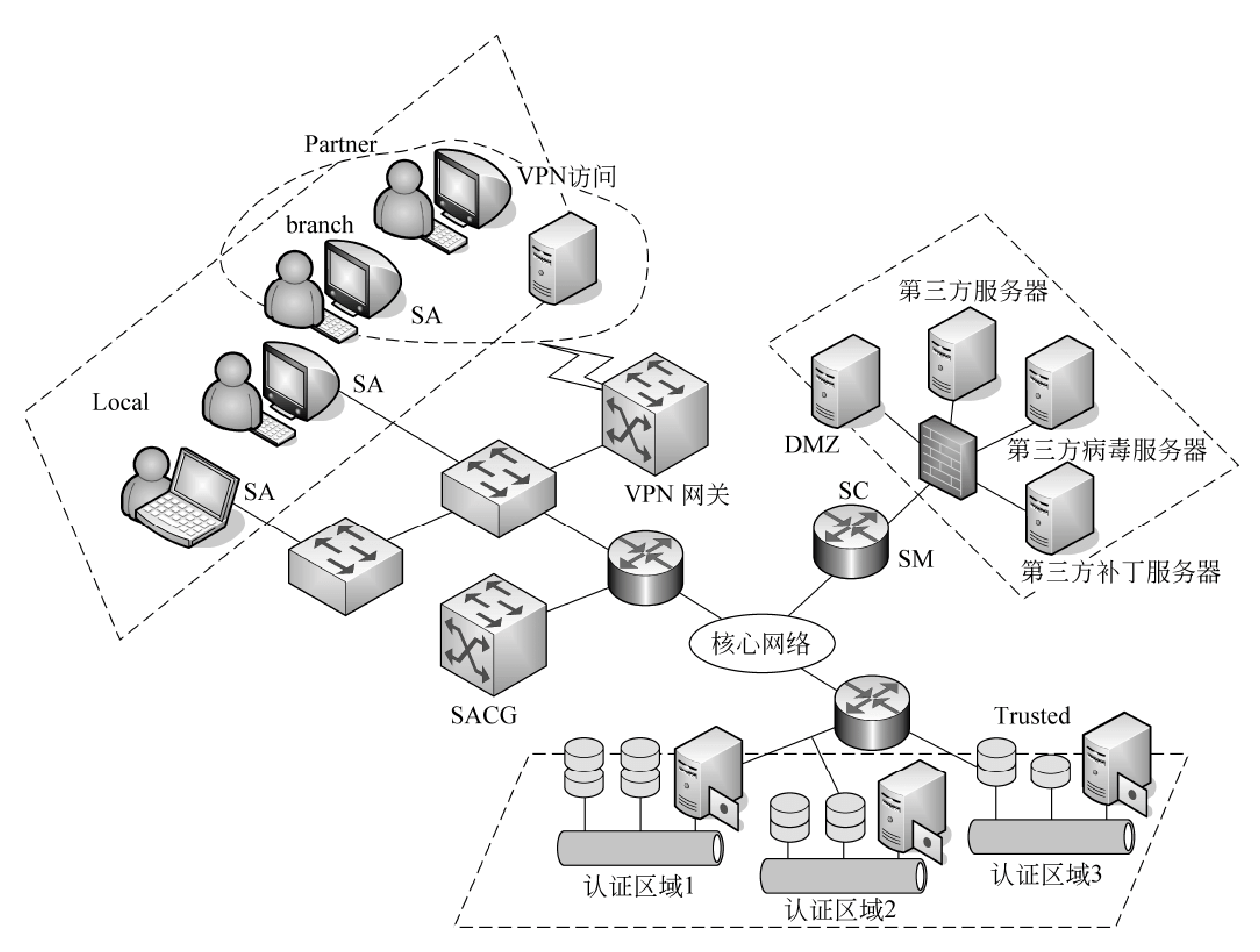


图 5.2　Secospace 终端安全管理的系统组成

网络中的资源被划分为前域、隔离域和后域。前域是指身份认证前可以访问的资源，如 DNS 服务器、外部认证源、业务控制器。隔离域是指用户通过了身份认证但未通过安全认证时允许访问的区域，如补丁服务器、防病毒服务器。后域是指用户通过安全认证后才能访问的区域，如 ERP 系统、财务系统、数据库系统。

5. 华为 Secospace 终端安全管理

ACG 安全接入控制网关，是实现接入控制与访问控制的核心设备，根据用户组来控制对业务服务器的访问权限，进行实时控制。

电信级的硬件平台，支持双机热备，高可靠性，实现细粒度的多认证后域划分，提供 3 个级别的设备支持不同的并发用户数(300/500/1000)。

6. Secospace 终端安全解决方案功能

Secospace 终端安全解决方案主要解决准入控制、终端安全基线管理、用户行为管理、补丁和软件的分发等功能。

准入控制是指发现并控制内部员工、外来访客和合作伙伴等对企业网络资源的访问，防止非法用户和不安全的终端接入内网，并根据用户身份授权访问指定的内网资源。

终端安全基线管理是指集中配置终端的安全基线，全面评估终端的安全状态，对不符合安全基线的终端进行隔离、修复，提高终端的安全防护水平，保证企业整网的安全。

用户行为管理是指审计并控制终端用户违反企业管理制度的行为，如 Web 访问、媒体下载、非法软件使用、非法外联、计算机外设、网络访问行为、网络异常监测等，防止计算机和网络资源的滥用和恶意破坏，规范终端用户使用 IT 资源的行为，提高企业整网的可用性和安全性。

补丁和软件分发是指提供智能、高效的补丁和软件分发功能，准确地评估系统漏洞，在最大限度降低网络带宽占用率的同时，及时帮助终端更新补丁，消除终端的安全漏洞；企业资产安全审计，动态收集企业软、硬件资产信息，跟踪企业资产变更，帮助管理员全面了解终端资产状况，提升企业整网的 IT 管理水平。

7. 安全接入控制为客户解决的问题

安全控制主要为客户解决：控制终端网络接入；访问权限管理；针对不同场景提供灵活的接入控制的问题。

(1) 控制终端网络接入，保障内部网络安全。禁止非授权的终端进入网络；禁止不安全的终端进入网络；禁止违规的终端进入网络。

(2) 访问权限管理，保护企业核心资源。安全接入控制网关提供网络层访问权限控制；支持划分多认证后域，实现细粒度访问权限管理。

(3) 针对不同场景提供灵活的接入控制方式。终端代理＋安全接入控制网关；Web＋安全接入控制网关；终端代理＋802.1X；终端代理＋802.1X＋安全接入控制网关。

5.2.2 接入控制方式

1. 安全接入控制网关方式及特点

安全接入控制网关 SACG 是 Secospace 主推的接入控制方案，该方案同 802.1X、DHCP、ARP 等方式相比优势明显。安全网关是各种技术有趣的融合，具有重要且独特的保护作用，其范围从协议级过滤到十分复杂的应用级过滤。防火墙主要有三类，分别为分组过滤、电路网关、应用网关三类。安全网关在应用层和网络层上面都有防火墙的身影，在第三层上面还能看到 VPN 作用。安全接入控制网关 SACG、电信级硬件网关设备，提供对终端的安全接入控制，部署和维护简单，安全可靠、性能卓越。

SACG 是由一个路由器和一个处理机构成的安全网关，两个部件结合在一起后，它们可以提供协议、链路和应用级保护。这种专用的网关不像其他种类的网关一样，需要提供转换

功能。作为网络边缘的网关，它们的责任是控制出入的数据流。显然，由这种网关连接的内网与外网都使用 IP 协议，因此不需要做协议转换，过滤是最重要的。保护内网不被非授权的外部网络访问的原因是显然的。控制向外访问的原因就不那么明显了。

SACG 是在华为电信级防火墙硬件平台上开发的专用的接入控制网关，通过基于角色的 ACL 规则（UCL）动态将用户关联到可以访问的认证后域，未通过身份认证和安全检查前，使用认证前域对应的 ACL 规则进行数据包的过滤，限制用户访问的网络资源。

安全接入控制网关方案的最大优点是可实现基于角色的网络访问权限控制；而且部署和实施简单，采用侧挂或直挂的方式，不改变现网拓扑结构。

电信级的安全标准，服务器支持资源池方式，SACG 双机热备支持逃生道，SC 与 SACG 维持心跳，当服务器异常时 SACG 可自动根据业务优先或安全优先，开放或关闭所有网络权限控制。

安全接入控制网关方式的特点是：基于用户角色的访问权限控制；不改变现网拓扑结构，部署维护简单；电信级安全标准，高可靠性；支持逃生通道，可自动恢复故障。

SACG 接入认证的原理和流程如图 5.3 所示。

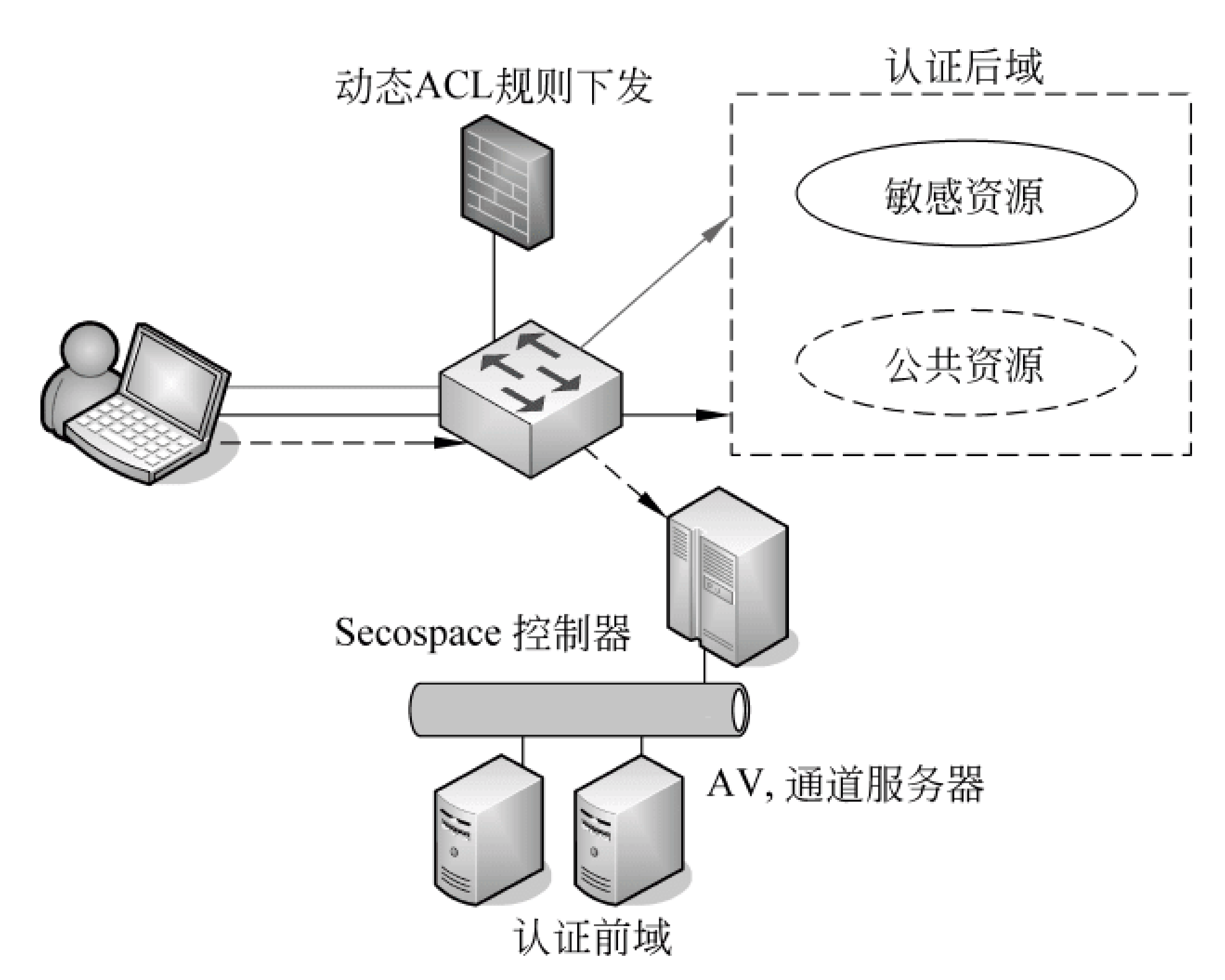


图 5.3　安全接入控制网关方式

（1）用户终端接入企业标准网络时，Secospace 代理会与 SC 控制服务器建立一个 SSL 通道，用于保护 Secospace 代理 SA 和服务器之间的通信。

（2）SA 与服务器协商认证的参数以及 License 控制信息，进行 Liscense 验证。

（3）执行身份认证流程。SA 根据采用的身份认证类型（用户名＋口令/AD 域集成认证等），将用户名/口令信息上报至服务器进行身份认证；如果是域认证方式（如 AD\ED 和第三方 LADP 系统等），Secospace 将与域管理服务器联动，使用域系统作为统一第三方认证源，用户无须再次输入用户名/口令即可成功认证。

（4）SA 向服务器请求更新安全策略，获得最新的策略信息列表，根据策略执行本地安全策略检查，最后将结果上报 SC。

（5）SC 收到安全认证的结果，判断是否符合策略规定的接入要求，如果满足，则与 SACG 联动，通过用户的身份属性匹配 ACL 规则，把对应的终端从认证前域切换到认证后

域，实现最小授权访问的目的；用于保护 Secospace 代理 SA 和服务器之间的通信。

2. 802.1X 接入控制方式

802.1X 是一种基于端口的网络接入控制技术，起源于 802.11 协议，制订 1X 协议的初衷是为了解决无线局域网用户的接入认证问题。

在它的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能，从而可以实现业务与认证的分离，SC 和以太网交换机利用不可控的逻辑端口共同完成对用户的认证与控制，业务报文直接承载在正常的二层报文上通过可控端口进行交换。802.1X 接入控制方式简化了 PPPOE 方式中对每个数据包进行拆包和封装等烦琐的工作。所以 802.1X 封装效率高，消除了网络瓶颈，对设备的整体性能要求不高，可有效降低建网成本。

Secospace V1R2 C02 中与数通交换机联动，通过对动态 VLAN 和动态 ACL 规则下发的支持，解决不同用户角色的访问权限控制，并能隔离不安全终端到隔离域接受安全修复，解决 R1 版本 1X 方案的局限。

如图 5.4 所示，新的 1X 方案中增加了隔离域的概念，不仅能防止不安全终端对后域的威胁，同时能起到保护其他未通过认证终端的作用。1X 的另一个优点是安全性较高，抗攻击力强，认证通过前端口处于关闭状态，使终端无法访问认证后域。但是 1X 也有其固有的局限性，由于要在每台交换机上做配置，实施和日常维护相对复杂；因为存在单点故障，方案的可靠性不高，故障恢复需要手动关闭 1X。

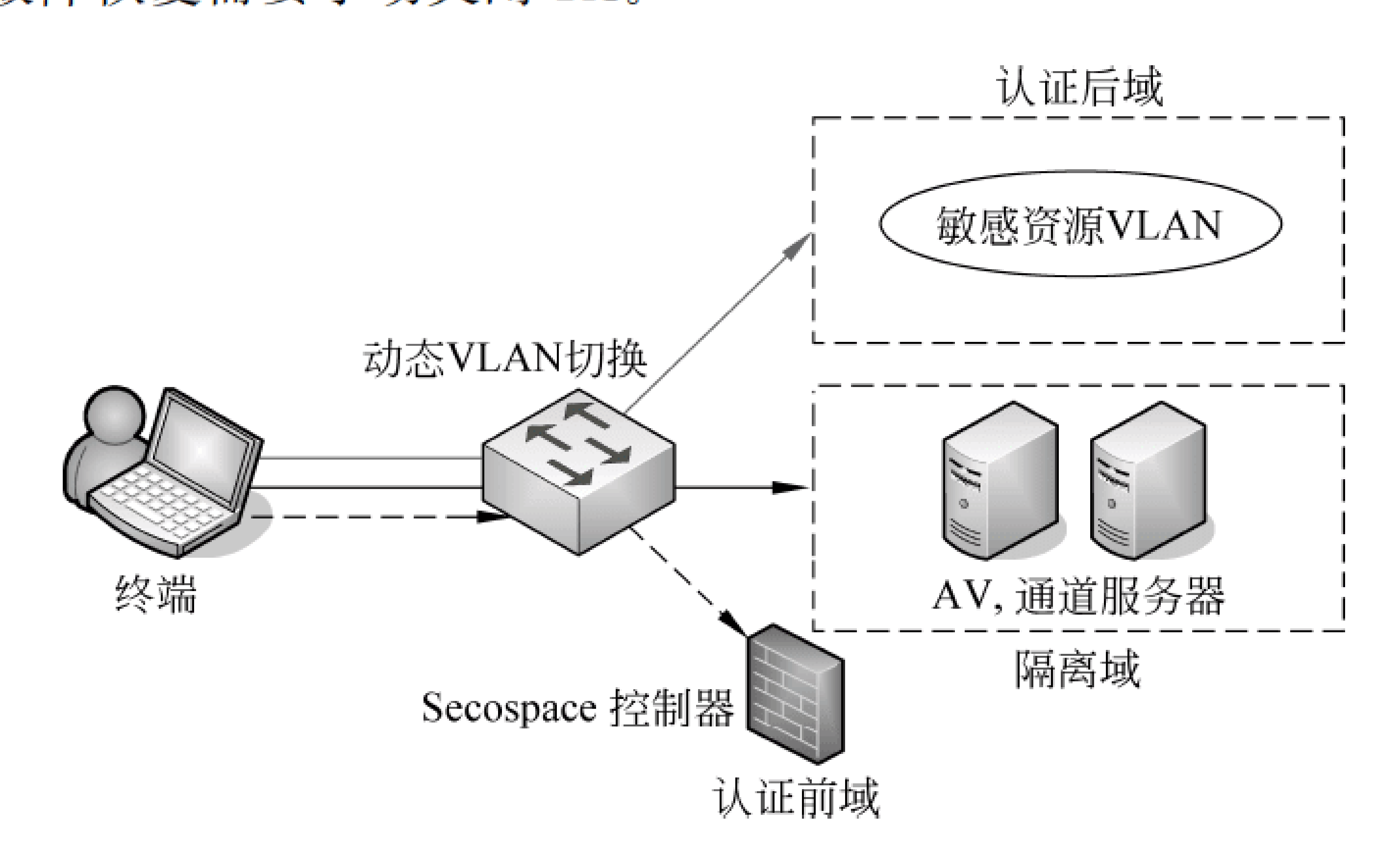


图 5.4　802.1X 接入控制方式

因此，该方案适用于网络规模较小，物理位置相对集中的场景；要求接入层设备都支持 802.1X 协议；可以满足内部员工、临时雇员和合作伙伴的接入控制；对管理员的网管水平要求高。

802.1X 接入控制方式的特点是二层协议，对设备的整体性能要求不高，可有效降低建网成本。基于用户角色的访问权限控制（动态 VLAN、ACL 下发）；认证与业务分离，安全性高，认证通过前无法访问网络；提供隔离域，防止威胁其他终端。

3. 主机防火墙接入控制方式

主机防火墙接入控制方式是 Secospace V1R2C 01 中实现的核心功能点，方案设计的应用场景是与 SACG 控制方式结合，提供有效的局域网内终端的互访控制。当然，该方案也可独当一面，通过单独部署实现独立的网络准入和终端互访保护。

主机防火墙接入控制方式适用于网络层次不太清晰、服务器分散的中小型网络。内部员工、临时雇员、合作伙伴要求部署和维护工作量投入有限，如图 5.5 所示。

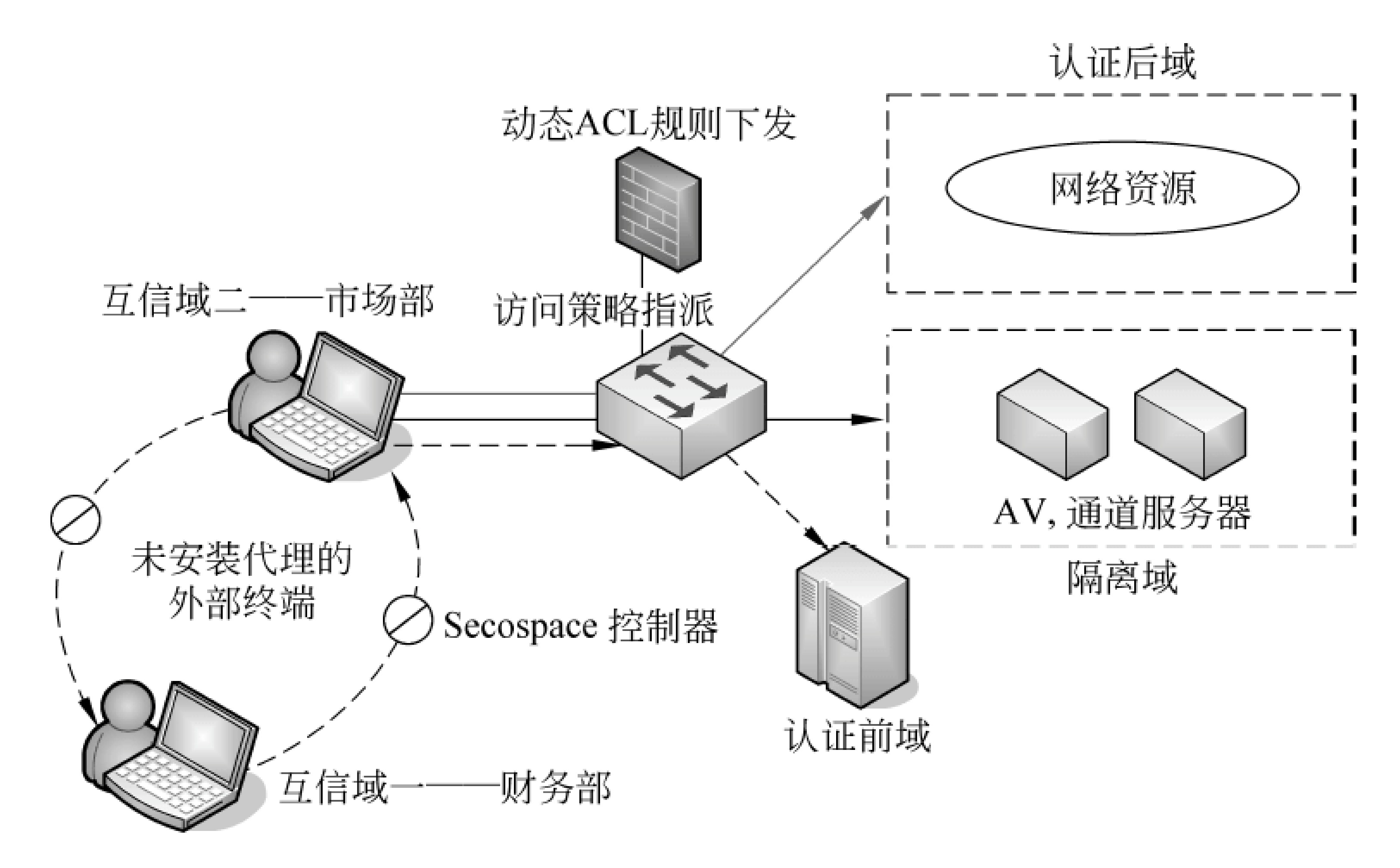


图 5.5 主机防火墙接入控制方式

主机防火墙接入控制方式的特点是有效控制局域网内终端互访行为；提供隔离域，防止威胁其他终端；纯软件控制方式，效率高，配置灵活，部署和维护简单；支持逃生通道，可自动恢复故障。

4. 不同场景和角色实现网络接入保护

主机采用硬件安全接入网关方式接入网络，旁挂在汇聚层交换机上，安装了 Secospace 代理的市场部员工，在通过身份认证和安全策略检查后可正常接入网络，访问企业的公共资源；财务部员工终端上没有安装代理，由 SACG 提供 Web 推送功能，当员工打开浏览器访问网站时，可通过 URL 重定向的方式重定向到定制的 Web 页面上下载 Secospace 代理，员工安装 SA 后即可通过接入控制流程，最终获取相应资源的访问权限，如图 5.6 所示。

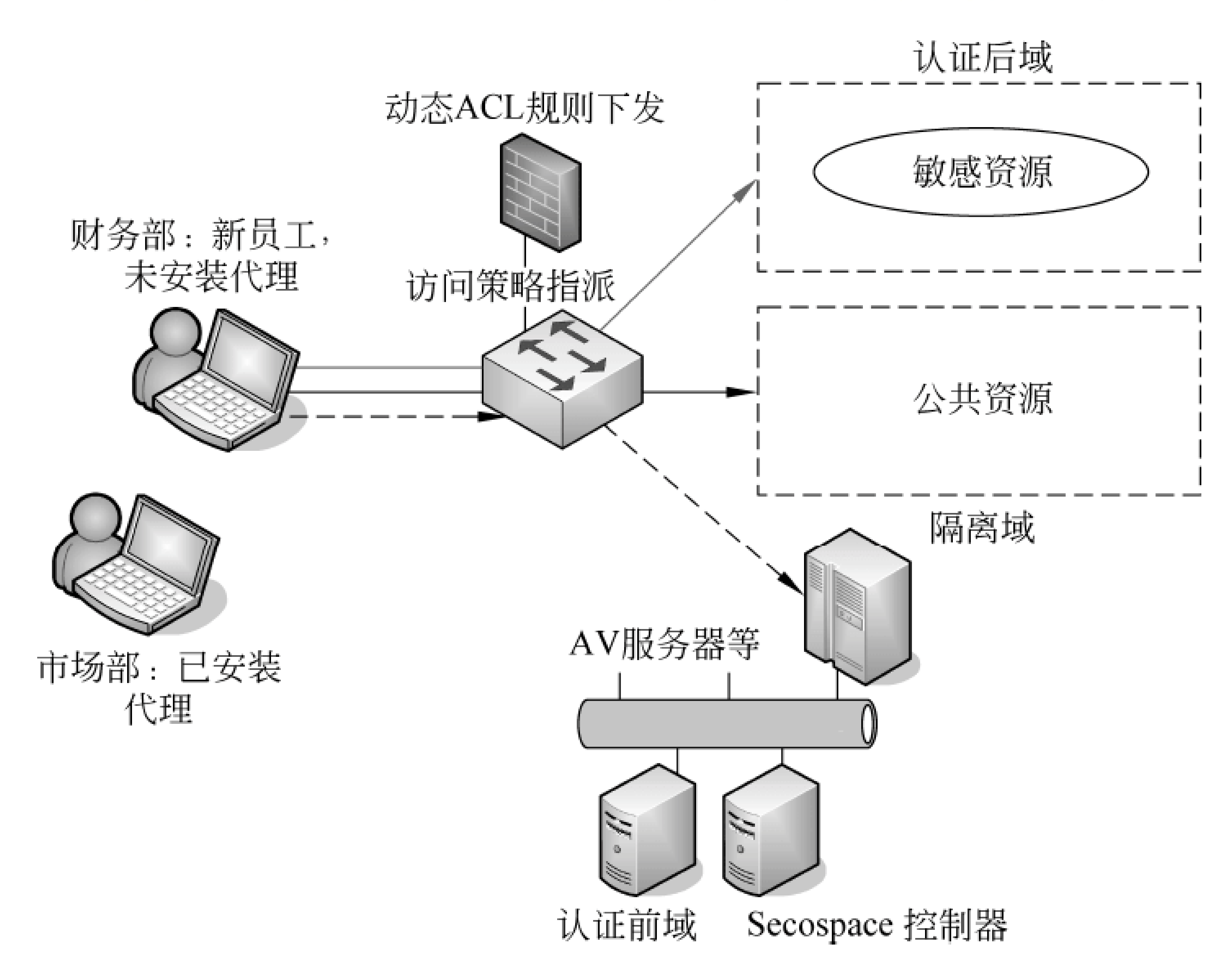


图 5.6 硬件安全接入控制网关方式

在这里了解到 Secospace V1R2 C01 中实现的又一亮点：支持 CA 认证，用于鉴别用户身份，Secospace 可支持所有遵循 X.509 标准的数字证书，可以很好地满足目前研究所、金融和涉密单位的需求。

同样，Secospace V1R2 C01 还可采用主机防火墙接入控制方式，通过指派 IPSec 策略，建立不同互信域，如财务部终端作为互信域 1、市场部作为互信域 2，即使都通过了安全检查，不同互信域间也不可互访。与此同时，对于未安装代理的外部终端或未通过身份认证和安全检查的非可信终端也不可访问通过安全检查的可信终端。这样就能有效阻止不安全终端对安全终端的互访行为，如共享目录就能够使局域网中的设备免遭病毒及蠕虫等攻击。

最后还可采用 802.1X 接入控制方式，未通过身份认证和安全检查前，交换机端口处于关闭状态，终端不可访问局域网内的领域终端，检查通过后通过交换机动态切换 VLAN，控制终端可访问的认证后域，实现基于不同用户角色的网络访问控制，如图 5.7 所示。

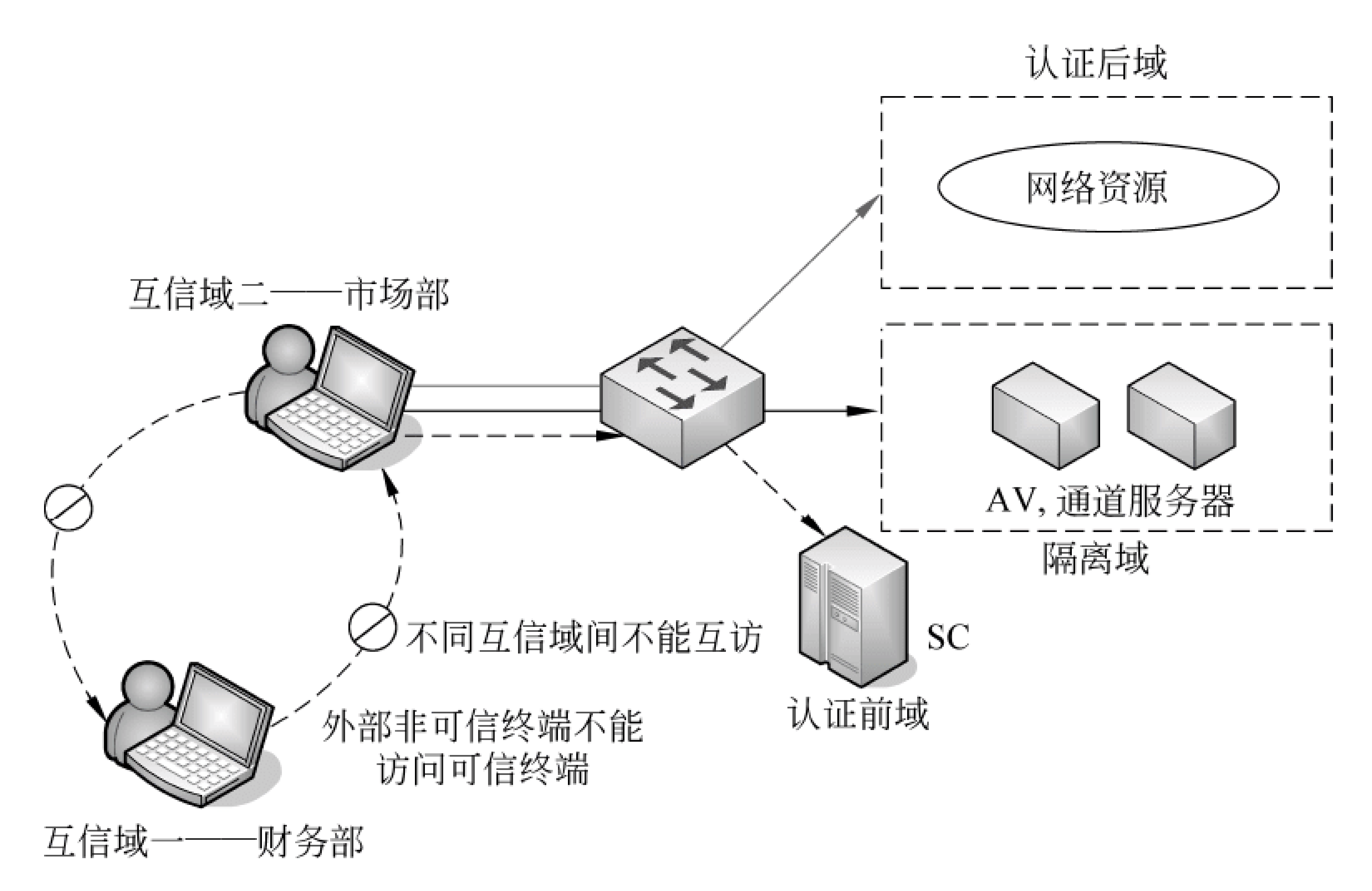


图 5.7　主机接入防火墙控制方式

下面描述用户非常关注的临时访客接入场景。这也是 Gartner 研究报告调查显示 80% NAC 项目的第一驱动因素：如何为访客提供安全的内部网络服务？

在这里推荐通过 SACG＋ActiveX 或 Web 的接入控制方式。一般临时访客的接入方式比较多样，如通过网线直接接入公司内部网口或交换机，或者通过无线网卡接入。由于临时访客往往不愿意安装代理，Secospace V1R2 C01 提供了 ActiveX 认证，用户只需要通过 SACG 提供的 URL 重定向下载 ActiveX 控件，迅速通过访客公共账号实现接入。如果用户的操作系统是 Mac 或者 Unix，也可通过 SACG 提供的 URL 重定向进行 Web 认证。但是要注意 Web 认证方式只能实现单纯的身份认证和接入控制，由于终端没有代理，安全策略检查和后面将要介绍的员工行为管理、资产管理等都无法实现。但这对于满足访客的内网接入控制需求足矣。

最后是远程办公、合作伙伴 VPN 接入场景。同样采用 SACG＋ActiveX/Web 的接入控制方式，在用户通过 VPN 接入后，SACG 分别给合作伙伴或远程办公用户提供 Web 推送，通过 URL 重定向下载 ActiveX/Secospace 代理，或直接通过 Web 认证方式接入。但要注意远程办公、合作伙伴 VPN 接入要求 VPN 没有做 NAT 网络地址转换；否则就会出现一

个用户通过认证，其他 VPN 用户都可以直接接入网络的情况。

5.2.3 华为终端管理安全管理策略与安全性检查

安全策略管理和员工行为管理也是 Secospace 相比于友商的突出优势。Secospace 提供业界最丰富的安全策略，各类检查类、网络行为监控和移动存储、外设管理等，全面评估端点安全状态，强制企业 IT 策略遵从，并持续监控，主动消除各种已知和未知威胁，如财务部由于经常访问企业敏感的财务信息，可以制定严格的安全策略模板，实行严格的策略检查和准入，防止恶意攻击。总裁办公室则可制定相对宽松的安全策略模板，满足基本的准入条件即可接入企业标准网络。

业界最丰富的安全策略是强制企业 IT 策略遵从主动评估终端安全状态，强制终端策略遵从。自动发现终端漏洞，消除已知和未知威胁。量体裁衣，基于角色的动态管理策略控制方式是根据用户角色或部门自定义不同安全规则，针对不同控制点采取的不同策略。那么安全策略管理为客户解决的问题又有哪些呢？像人性化的安全策略管理（灵活选择实施的安全策略内容；灵活选择策略执行类型为强制或非强制；灵活选择策略实施对象），全面的企业安全策略，全面提升企业信息安全水平，提高效率等。

终端安全性检查可以由审计人员通过下达审计监控任务，对用户终端的安全性状况进行检查，并生成审计报表；也可以由用户发起进行本机自检，显示出来检查结果，让用户了解本机安全状况，帮助用户提高本机安全性，防止无意泄密。

华为终端安全性检查的基本流程依次为：获取计算机终端基本配置信息、检查分区表信息、检查共享目录、获取终端硬件信息、获取终端进程信息、检查屏保设置信息、检查安装软件、检查 Windows 补丁、检查其他软件补丁。

那么，如何进行华为终端安全性检查呢？首先要获取计算机终端的基本配置信息、检查分区列表和共享目录，获取终端硬件信息和进程信息，之后再检查屏保设置信息，信息无误后安装软件和 Windows 补丁，安装完成后进行防泄密检查，并用 USB 存储设备监视，最后进行屏幕监控。下面来看一下具体的操作步骤。

（1）获取计算机终端基本配置信息。可以获得机器的 IP 地址信息、MAC 地址信息、主机名、操作系统版本信息。

（2）检查分区表信息。可以检查分区数量，分区大小，分区类型，是否隐藏分区。如果有违规分区将用红色显示。

（3）检查共享目录。可以检查共享名，共享目录路径，是否设置密码。如果有违规目录将用红色显示。

（4）获取终端硬件信息。可以获取机器的基本硬件配置信息。

（5）获取终端进程信息。可以获取机器目前的进程信息。

（6）检查屏保设置信息。可以检查屏保是否设置密码，屏保启动时间，根据策略判断启动时间是否符合要求；如果有不符合策略文件的将用红色显示。

（7）检查安装软件。可以通过注册表检查已安装的软件，根据策略文件判断软件为合法、非法等类型。如果缺少必装软件或有违规软件将用红色显示。

（8）检查 Windows 补丁。通过注册表检查已安装的 Windows 补丁，根据策略文件判断有没有没装的要求补丁。如果没有将用红色显示。

（9）检查其他软件补丁。可以通过注册表检查 SQL Server、Office 的补丁。

（10）防泄密检查。此类检查只能由审计人员下达审计监控任务，在后台对用户终端进行检查，生成审计报表。防泄密检查的基本流程依次为检测文件类型的特征码、搜索文档的关键字、搜索邮件的关键字、上网历史记录、搜索游戏软件、USB 存储设备监视、MODEM 拨号监视。

（11）检测文件类型的特征码。检查可能被更改过扩展名的文件的路径以及此文件可能的原类型信息。所有查到的结果文件都将用红色显示。

（12）搜索文档的关键字。搜索结果包括了目标计算机上所有包含符合搜索逻辑的关键字的 Doc 文档和 txt 文档的路径和它们所包含的关键字信息。所有搜索到的结果都将用红色显示。

（13）搜索邮件的关键字。搜索结果包括了目标计算机上 Outlook Express 和 Foxmail 邮件工具中所有包含符合搜索逻辑的关键字的邮件信息。所有搜索到的结果都将用红色显示；获取上网历史记录：搜索结果包括了目标计算机近期上过的网站地址的记录。如果目标计算机的网站地址记录中存在审计策略中声明的违规网站，那么这些违规网址将用红色显示。

（14）搜索游戏软件。搜索结果包括了目标计算机上所有可能的游戏软件的信息，且结果用红色显示。

（15）USB 存储设备监视。当打开 USB 存储设备监视时，所有 USB 存储设备的使用都将被记录下来，并上传服务器，且结果用红色显示。

（16）MODEM 拨号监视。当打开 MODEM 拨号监视时，所有 MODEM 拨号都将被记录下来，并上传服务器，且结果用红色显示。

（17）屏幕监控。当打开屏幕监控后，使用远程监控控制台软件连接目标计算机，就可以查看计算机的屏幕显示。

5.2.4 Secospace 在移动存储介质和外设管理上的控制

移动存储介质管理 PSM 将作为 Secospace TSM 的组件构筑 IT 内控解决方案的标准。在 V1R2 C02 中将实现 PSM 和 TSM 两个代理的融合。目前 PSM 在实现融合前将提供少量的独立销售。

PSM 提供了完善的移动存储介质管理功能，有效解决日趋流行的各类 USB 移动硬盘、智能手机、FLash Disk、USB MP3/4 MODEM 蓝牙等的违规使用，避免引入的信息泄密风险。PSM 实现的主要功能包括以下几种。

（1）注册管理，限定只有注册过的设备才能在内网使用。

（2）控制权限包括基本的读、写、复制控制，同时可提供加密设备的功能，为敏感文件提供加密保护。

（3）在事后的全面操作审计，如详细的复制文件、设备插拔记录等。

另外，对于终端本地的进程和服务也能提供黑白名单控制功能，可通过定义强制运行的信息安全软件，如反间谍、反木马软件等阻止恶意攻击，强制关闭危险的服务和进程，减少攻击者的渗透风险。最后还能进行本地文件操作监控、外设接口管理等。另外，值得关注的是 Secospace V1R2 C01 中还将实现对 USB 蓝牙、USB 红外、USB 无线网卡的控制。

上述所有策略基本都能支持离线运行，对各种违规行为的控制手段也可根据用户需求灵活设置，如配置为及时阻断或分时间段阻断，或者只记录违规行为，作为事后审计的需求。

用户安全接入网络后，Secospace 会提供持续的员工行为审计，解决 CIO 最关注的非法外联、P2P 下载、ARP 攻击和移动存储设备管理等问题。保障企业内网的可用性和效率，全面防止信息泄密、网络滥用问题以及网络层和应用层的恶意破坏。首先看一下 Secospace 在非法外联上的严密控制，通过探测正常的外联是否经过特定网络出口，可对非法假设的代理服务器等进行记录并上报服务器。同时，如果用户是通过 Windows 拨号连接，如 MODEM、ASDL、ISDN、PPPOE 或 VPN 连接，Secospace 可及时断开这些连接，并将违规记录上报。另外，如果用户试图通过多网卡进行非法外联，Secospace 也可实时监测，并可与 SACG 联动禁止终端接入网络。

对于令 CIO 最头疼的 IM、炒股软件、P2P 下载和网游等，Secospace 也可在进程访问网络时及时阻断会话。同时对于用户的网络流量也可灵活地基于协议和端口进行控制，协议类型包括 TCP/UDP/ICMP/HTTP/SMTP/Netbios 等，并可设置一般违规阈值和严重违规阈值，以及设置周期进行统计，上报服务器，而且该策略能支持离线运行。

最后对于 Web 访问和 IP 访问也有严格控制，可通过设置过滤各种恶意、可疑网站如钓鱼、僵尸网络的网站访问，避免终端接触各种恶意链接；通过配置主机防火墙的 IP 规则，可有效阻止应用层的信息泄密和其他安全风险，如 SMTP、FTP、Telnet 控制等。

补丁管理为客户端解决的问题如下。

(1) 自动补丁检查和加载。可根据检查情况自动从 SRS 上下拉需要的补丁以及自动安装；智能化补丁管理等。

(2) 智能化补丁管理。管理员只需要维护修复服务上的补丁，补丁检查、下发、安装完全自动化；支持管理员从服务器端手动分发补丁，可设置分发的终端；还可以智能识别网络状态，选择网络空闲时分发补丁。

(3) 终端自动检查补丁状况。识别需要更新的补丁，自动从修复服务器(SPS)上下拉需要完善的补丁，自动安装，用户无感知。

(4) 智能化补丁管理。管理员只需要维护修复服上器的补丁，其他的补丁检查、下发、安装完全自动化；同时也支持管理员从服务器端手动分发补丁，可设置分发的终端；可智能识别网络状态，选择闲时分发补丁。

Secospace 终端安全解决方案为企业带来了很大的优势，不仅实现立体的企业内网安全防护、终端认证和安全检查、硬件 SACG 实现网络层访问控制、细粒度的授权管理保障业务系统安全，还帮助企业提升信息安全管理水平、全面的安全策略检查和灵活的安全策略管理，帮助企业进行员工违规行为审计和员工行为管理。最终还为客户提供 SACG 支持双机热备，满足电信级可靠标准和 SC 支持负载均衡保障的终端管理方案。

5.2.5 实例

案例 5.1 解决安徽电信 DCN 内网安全管理。

安徽省由于地市众多，所以电信 DCN 非常庞大，包括 17 个地市 DCN、省中心 DCN。

在项目中华为公司以 DCN 安全域划分理论为指导，基于在通信领域的核心技术积累和业务网络的理解，依靠自身丰富的通信网络服务经验和广泛的合作伙伴提供了安徽电信 DCN 安全解决方案。

在安全域理论认为最容易形成安全短板的终端用户域，华为公司采用接入认证＋安全

策略强制技术进行了重点防护，具体产品包括 19 台 5200F、华为终端安全策略强制系统，对安徽电信 17 个地市 DCN 和省中心 DCN 共计 15000 终端进行了防护。

迄今为止，安徽电信 DCN 安全项目是华为终端安全解决方案终端数量、5200F 部署数量最多的重要案例之一。

Secospace 终端安全解决方案：以接入控制技术为核心，策略强制为纽带，通过网络和系统两个层面来搭建终端安全管理平台，将现有终端的补丁管理、软件分发、资产管理、信息安全等相关技术进行整合，达到技术支撑对管理的有效辅助。华为的终端安全管理解决方案的建设使得用户在信息化后的高效工作中不再担心病毒、黑客、内部信息泄密的烦扰，有力保障了安徽电信 DCN 内 2.5 万终端的安全。

案例 5.2 为中国移动提供终端安全管理。

作为中国规模最大的移动通信运营商，雄居全球运营商榜首市值过千亿美金，中国移动既要面对外界的审核又要不断提升内部的管理，使得其对自身的内网安全提出了更高的要求。

Secospace 终端安全解决方案：2006 年中国移动通过严格测试和比较，最终选择了华为的终端安全管理系统为其全国近 8 万个 OA 办公终端提供终端安全保护。华为的终端安全管理解决方案的建设使得用户在信息化后的高效工作中不再担心病毒、黑客、内部信息泄密的烦扰，有力保障了中国移动的业务发展。

案例 5.3 打造福建兴业银行内网安全防护体系。

没有 IT 技术平台的支撑，银行的内网安全就无法进行有效的管理和防范，各种终端都可能有意无意地对银行的业务系统造成不利的影响。随着兴业银行各项业务的迅猛发展，内部网络的信息安全建设和运维都是摆在银行管理者面前的一个难题。

Secospace 终端安全解决方案：终端安全管理解决方案为兴业银行建立内网安全防护体系。文档权限安全为用户的信息资产提供防主动泄密解决方案。内网安全防护体系的建设使得用户在信息化建设后免受病毒、黑客等的攻击和干扰，并且有力保障了文档资料的安全，从而为银行系统正常的业务开展提供了内网安全平台。

案例 5.4 助力东方锅炉应对 SOX 审计。

作为上市公司，东锅集团需要接受国际级审计公司对 SOX 法案各项严格安全规定的审计，同时东锅集团内部需要在信息安全管理整体上一个新台阶。

Secospace 终端安全解决方案：信息安全咨询和评估服务帮助用户制订信息安全管理改进规划；终端安全管理解决方案为东锅集团信息安全管理制度的落实提供有效的技术保障。通过有效的信息安全建设和管理经验的传递，帮助东锅集团快速构建了全面、高效的信息安全管理平台，在面对内部安全管理与外部安全审计时都有了十足的信心，有力保障了主营业务的顺利发展。

5.3 H3C 终端接入控制解决方案

5.3.1 整体方案介绍

H3C 终端接入控制解决方案（End user Admission Domination，EAD）从控制用户终端安全接入网络的角度入手，整合网络接入控制与终端安全产品，通过智能客户端、安全策略

服务器、联动设备以及第三方软件的联动，对接入网络的用户终端按需实施灵活的安全策略，并严格控制终端用户的网络使用行为，极大地加强了用户终端的主动防御能力，为IT管理人员提供了高效、易用的管理工具。

对于要接入网络的用户，EAD解决方案首先要对其进行身份认证，通过身份认证的用户进行终端的安全检查，根据IT管理员制定的安全策略进行。策略包括病毒库更新情况、系统补丁安装情况、软件的黑白名单等内容的安全检查。根据检查的结果，EAD对用户网络准入进行授权和控制。通过安全认证后，用户可以正常使用网络。与此同时，EAD可以对用户终端运行情况、网络使用情况和资产情况进行审计和监控。

EAD解决方案组件包括智能客户端、联动设备、安全策略服务器和第三方服务器。下面详细介绍这4种服务器的作用。

(1) 智能客户端是指安装了H3C iNode智能客户端的用户接入终端，负责身份认证的发起、安全策略的检查以及和安全策略服务器配合进行终端控制。

(2) 联动设备是网络中安全策略的实施点，起到强制用户准入认证、隔离不合格终端、为合法用户提供网络服务的作用。根据应用场合的不同，联动设备可以是交换机、路由器、VPN网关或无线设备，分别实现不同认证方式(如802.1X、VPN和Portal等)的终端接入控制。针对多样化的网络，EAD提供了灵活多样的组网方案，联动设备可以根据需要进行灵活部署。

(3) 安全策略服务器是EAD方案中的管理与控制中心，兼具终端用户管理、安全策略管理、安全状态评估、安全联动控制以及安全事件审计等功能。

(4) 第三方服务器是指补丁服务器、病毒服务器等，被部署在隔离区中。当用户通过身份认证但安全认证失败时，用户将被隔离到隔离区，此时用户能且仅能访问隔离区中的服务器，通过第三方服务器进行自身安全修复，直到满足安全策略要求为止。

H3C终端接入控制解决方案的步骤是首先接入网络的用户需要进行认证(包括802.1X或者Portal认证)；如果认证通过，接入交换机根据用户身份下发ACL或者VLAN；然后访问相应的网络资源。

H3C终端接入控制解决方案的特点是接入交换机可以执行802.1X认证，认证通过后根据用户身份下发ACL进行动态访问控制。这种部署方式不改变网络结构，不存在网络迂回和单点故障问题。接入交换机即可实现认证、访问控制一体化控制。该方案的优点在于结构简单、部署方便。

随着EAD解决方案的不断发展，新特性、新功能层出不穷。以不断提供易用性和实用性、不断提高客户满意度为出发点，EAD解决方案已经在不知不觉中发生了较大的变化。客户也意识到对内网终端进行控制和管理的必要性，就目前来说，实施网络接入控制，确保企业网络安全，已是许多企业网客户的迫切需求。

EAD解决方案集成了网络准入、终端安全、桌面管理三大功能，帮助维护人员控制终端用户的网络使用行为，确保网络安全。

EAD在用户接入网络前，通过统一管理的安全策略强制检查终端用户的安全状态，并根据对终端用户安全状态的检查结果实施接入控制策略，对不符合企业安全标准的用户进行“隔离”，并强制用户进行病毒库升级、系统补丁升级等操作；在保证终端用户具备自防御能力并安全接入的前提下，可以通过动态分配ACL、VLAN等合理控制用户的网络权限，从

而提升网络的整体安全防御能力。

5.3.2 软件架构与安全级别

EDA 解决方案的软件架构的业务组件均基于 iMC 平台安装，用于实现各种业务。EAD 组件基于 UAM 组件安装。UAM 组件包含 RADIUS 服务器、策略服务器及策略代理服务器。EAD 组件包含 EAD 前台配置页面、桌面资产管理服务器及桌面资产管理代理。

EDA 解决方案的 4 种安全级别分别为监控模式、提醒模式、隔离模式、下线模式。

监控模式：无论安全检查结果如何，都提示用户通过安全检查，不弹出安全检查结果页面，不对用户做任何限制。只在服务器一侧记录检查结果以备之后审计。

提醒模式：若安全检查不通过则会提示用户存在安全隐患，但不对用户采取任何动作，不弹出安全检查结果页面。

隔离模式：若安全检查不通过，通知安全联动设备限制用户只能访问隔离区资源。

下线模式：若安全检查不通过，将用户强制下线。

1. 安全策略

引用安全级别，使能各项安全检查策略，配置动态 ACL 下发，除了使能这些安全检查策略之外，需要注意同时使能实时监控的功能。

服务是最终用户使用网络的一个途径，它由预先定义的一组网络使用特性组成，其中具体包括基本信息、授权服务是最终用户使用网络的一个途径，它由预先定义的一组网络使用特性组成，其中具体包括基本信息、授权信息、认证绑定信息、用户客户端配置和授权用户分组等。

2. 分组

服务用户分组：用户分组不再和服务关联，而是只和操作员关联。针对特定的用户分组执行特定的策略。与指定用户分组关联的操作员才能管理该分组内的用户以及产生的相关用户信息。

业务分组：将一些个性化策略归入指定的业务分组，只有与该业务分组关联的操作员才能够管理该业务分组中的策略。

5.3.3 802.1X 认证流程

Supplicant System——通常为一个用户终端系统，该终端系统通常要安装一个客户端软件（如 H3C802.1X、Windows XP 自带的 802.1X 客户端），用户通过启动这个客户端软件发起 802.1X 协议的认证过程。为支持基于端口的接入控制，客户端系统还需支持 EAPOL 协议。802.1X 协议是基于 Client/Server 的访问控制和认证协议。它可以限制未经授权的用户/设备通过接入端口（Access Port）访问 LAN/WLAN。在获得交换机或 LAN 提供的各种业务之前，802.1X 对连接到交换机端口上的用户/设备进行认证。在认证通过之前，802.1X 只允许 EAPoL（基于局域网的扩展认证协议）数据通过设备连接的交换机端口；认证通过以后，正常的数据可以顺利地通过以太网端口，如图 5.8 所示。

Authenticator System——通常为支持 802.1X 协议的网络设备。该设备对应于不同用户的端口（可以是物理端口，也可以是用户设备的 MAC 地址、VLAN、IP 等），有两种逻辑端口，即受控端口和不受控端口。不受控端口始终处于双向连通状态，受控端口可配置为双向

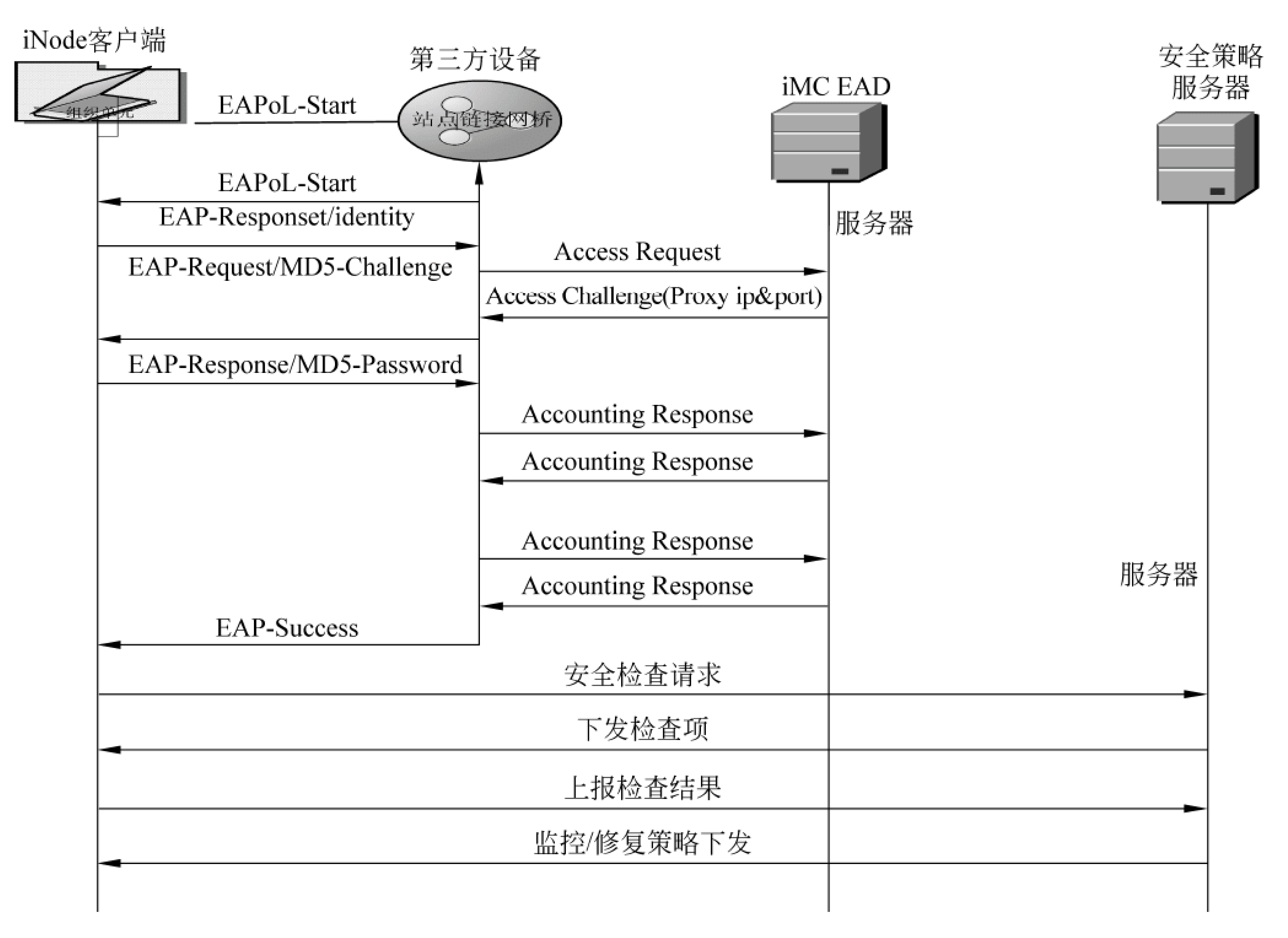


图 5.8　802.1X 认证流程

受控和仅输入受控两种方式,以适应不同的应用环境。如果用户未通过认证,受控端口处于未认证状态,则用户无法访问认证系统提供的服务。

Authentication Server System——通常为 RADIUS 服务器,该服务器可以存储有关用户的信息,如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等。当用户通过认证后,认证服务器会把用户的相关信息传递给认证系统,由认证系统构建动态的访问控制列表,用户的后续流量就将接受上述参数的监管。认证系统和认证服务器之间通过 RADIUS 协议进行通信。RADIUS 服务器是一个 AAA 协议,意思就是同时兼顾验证(Authentication)、授权(Authorization)及计费(Accounting)3 种服务的一种网络传输协议(Protocol),通常用于网络存取或流动 IP 服务,适用于局域网及漫游服务。RADIUS 服务器负责接收订户的连接请求、认证订户,然后返回客户机所有必要的配置信息以将服务发送到订户,如图 5.9 所示。

为了对终端用户的网络流量进行监控,EAD 解决方案支持异常流量监控特性。管理员设置终端用户流量阈值,iNode 客户端根据安全策略服务器的指令,打开流量监控功能,实现异常上报并根据安全策略服务器的指令对用户采取相应的动作。

检查防病毒客户端是否正常启动运行,病毒引擎和病毒库版本是否符合要求,与高级联动类型的防病毒软件联动,还支持设置病毒查杀策略等内容。与微软补丁服务器 WSUS Server 或 SMS Server 联动进行软件补丁检查(自动强制升级)。自定义系统软件补丁检查,可针对系统软件的不同版本自定义补丁检查策略。监控软件安装、进程运行和服务运行。

对于检查类型为“必须安装”或“必须运行”的可控软件组,只要安全检查结果匹配组内一条策略即认为检查通过;对于检查类型为“禁止安装”或“禁止运行”的可控软件组,只要安

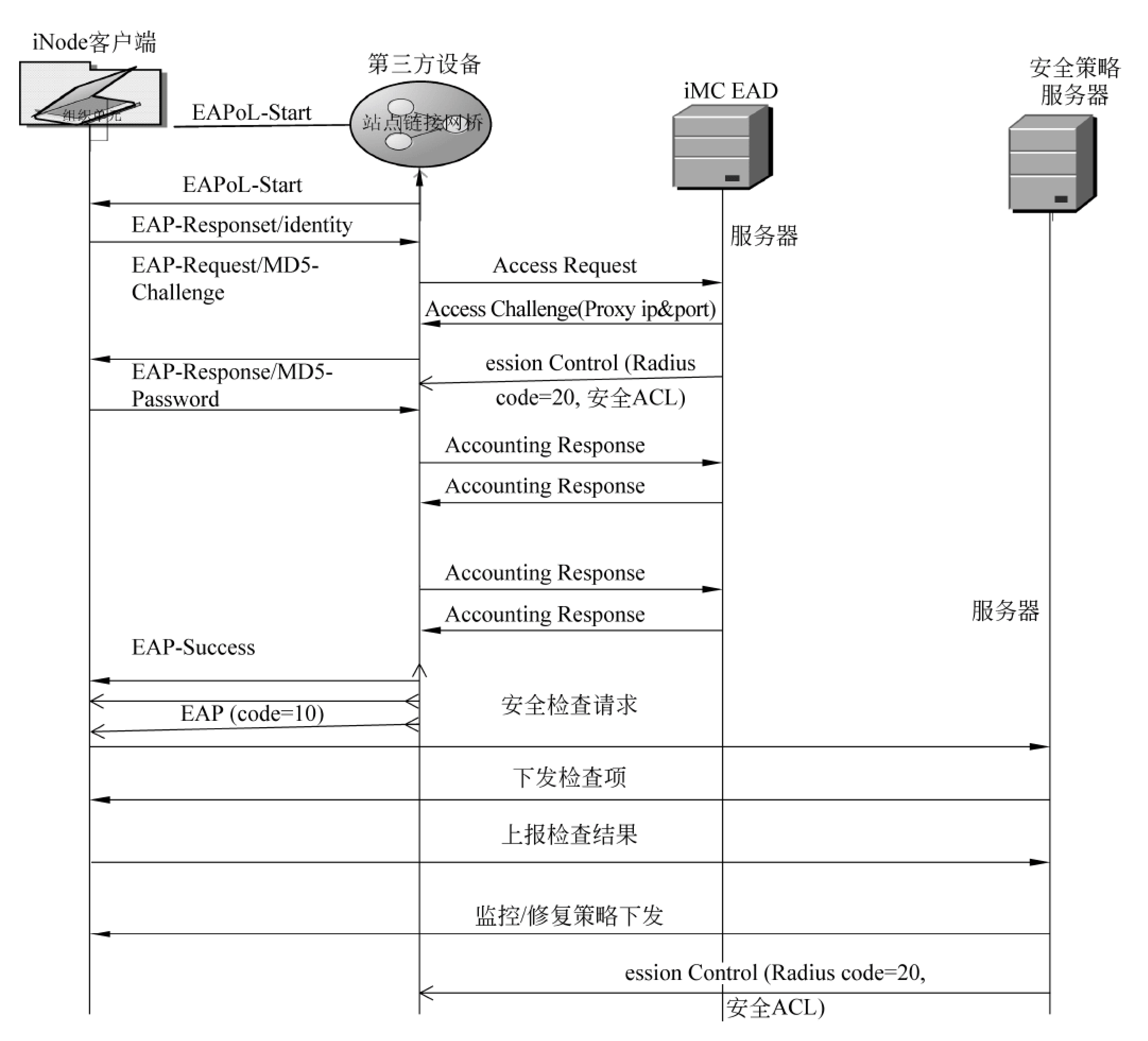


图 5.9　802.1X 认证流程

全检查结果匹配组内的一条策略即认为检查不通过。监控指定的注册表项中是否存在特性键名及键值。操作系统密码监控通过字典文件的方式，检查操作系统密码是否为字典文件中记录的弱密码。远程桌面连接提供了对在线用户进行远程登录的功能。网络管理员可以通过远程连接功能对远程终端用户的计算机进行维护和管理。

5.3.4　EAD 解决方案的容灾方案

1. 逃生工具

系用户接入逃生工具（简称为“逃生工具”）是 CAMS/iMC UAM 后台的替身。当 CAMS/iMC UAM 出现如进程宕掉、数据库异常、性能下降等故障无法处理认证或计费请求时，逃生工具暂时替代 CAMS/iMC UAM 处理请求报文以保障用户的业务不中断。逃生工具不验证用户信息与用户口令，不做绑定授权处理，也不启用安全认证，对于请求报文都直接回应成功。

逃生工具支持集中式部署（即和 iMC UAM 部署于同一台服务器上）和独立部署（单独部署在另一台服务器上）。逃生工具和 UAM 监听同样的端口，所以当集中式部署时只能启动两者之一。独立部署时，建议将逃生工具所在服务器配置成和原服务器一样的 IP 地址，

并离线放置。当出现故障时直接将原服务器的网线插到逃生工具服务器上，就好像替换备件。不建议配置不同的 IP 做主备切换。

逃生工具的优点：低成本的容灾方案，实施及维护非常简单；一种简单易行的附加保险，即使是使用了其他容灾方案，仍然可以准备一套逃生工具以备不时之需。

逃生工具的缺点：需要管理员及时发现故障并手动地切换使用逃生工具；用户业务仍然会中断；使用逃生工具期间，将损失认证用户的所有接入信息（日志、计费信息等）；由于逃生工具不对认证请求做任何判断，所以在使用逃生工具期间将存在一定的安全隐患。

2. BMAN 双机备份工作流程

系设备与主 iMC 服务器之间通信中断，发出的认证请求或计费请求在一定时间内未收到响应；自动将请求发往备 iMC 服务器，同时将主服务器状态置为 block；等待一定的时间间隔后，再次尝试将请求发往主 iMC 服务器，若通信恢复则立即将主服务器状态置为 active，从服务器状态不变。

DBMAN 双机备份方案的优点：双机自成一套完整的认证体系，能够解决所有的软硬件问题；双机切换期间，在还没有自动同步数据库之前用户数据库可以保留；实施及维护起来较方便。缺点：用户的业务仍然会中断。特定环境下，有可能发生交换机上计费服务器切换而认证服务器不切换的情况，从而导致 EAD 认证失败。

3. 双机热备

双机系统是至少两台计算机利用群集软件实现计算机备份冗余的方案，可实现应用的高可用性。群集是一个计算节点的集合，对外仅提供网络服务或应用程序（包括数据库、Web 服务和文件服务）的单一的客户视图。

SQL Server 数据库和 iMC 程序文件都安装在存储设备上，同一时间只会有一台 iMC 服务器使用共享磁盘阵列上的资源。两台服务器作为一个整体，对外提供一个虚 IP 作为 RADIUS 服务器的 IP 地址；通过群集软件（如 Windows 的群集管理器）保持两台 iMC 服务器之间的心跳，实时检测 iMC 相关的进程运行是否正常，当发生故障时自动将业务切换到另一台 iMC 服务器上。

双机热备的优点：真正的热备，对于终端用户来说切换不造成任何影响，没有业务中断的损失。对外相当于一台服务器，没有 DBMAN 双机模式下认证和计费报文发往不同服务器的隐患；能够解决 iMC 服务器本身的硬件故障。缺点：由于只有一套程序文件及数据存在，所以不能解决程序文件本身以及数据库本身的软件故障；实施及维护起来相对比较复杂。

5.3.5 安全工程能力成熟度模型

并非所有设备都支持 ACL 下发，设备的 ACL 资源有限，用户区分的角色越多设备上的 ACL 配置越复杂，无法通过服务器直接查看下发的 ACL 中所包含的具体规则。

传统的 RADIUS 方式下，EAD 心跳丢失服务器无法通过 RADIUS 报文通知第三方设备将用户下线。唯一的可能是直接清除在线表，在支持计费更新的环境下，等待设备下一次计费更新，然后返回会话时长为 0。但可惜第三方设备不支持会话时长为 0 的属性，所以即使是在支持计费更新的环境下清除在线列表也没有用，清除了反而使得管理员找不到哪些用户出现异常，所以传统的机制是将 EAD 心跳超时的用户在在线表中置为隔离状态。

RADIUS 身份认证通过后，客户端获取到安全检查代理的 IP 和端口后即发起安全认证。由策略服务器根据安全认证/心跳/下线报文维持在线表。UAM 后台对于计费报文或重认证报文仅做检测和回应，不再更新或删除在线表。通过 EAD 心跳回应报文返回用户剩余上网时长（接入时段限制、在线加入黑名单、用户被从在线列表中删除等），以精确控制在线用户。

1. 桌面资产管理

桌面资产管理（Desktop Asset Management）主要关注于企业的信息安全，可以对终端进行全方位的监控，保证用户只能合理合法地使用公司的信息资源，并提供实时和事后的审计。H3C 桌面管理模块可以提供丰富的桌面管理功能，包括以下几项。

（1）支持资产分组、资产编号自动生成、资产的增删改、支持手工扫描单个资产、自动关联资产责任人、资产信息上报策略定义、在线用户列表中查询资产信息。

（2）支持硬件、软件的资产变更管理，实时监控终端用户软件安装卸载/硬件变更状态。

（3）支持按照 CPU、操作系统、软件、资产类型、硬盘等信息提供资产统计功能。

（4）支持丰富的软件分发，其中包括按照资产批量分发软件、按照资产分组分发、立即分发软件和定时分发软件、按照分发任务查询每个资产的软件分发状态、支持资产的软件分发历史等。

（5）可对 USB 的使用进行监控，监控信息包括 USB 插拔记录、写文件名及文件大小等。对于 USB 的插拔记录可产生告警以提醒管理员注意。

（6）外置管理，实现对光驱、软驱、USB 移动存储、USB 全部接口（不包括 USB 鼠标、键盘）、打印机、调制解调器、串行口、并行口、1394 控制器、红外设备、蓝牙设备等进行启用和禁用。

2. DMA 架构与功能

DAM Agent 驻留在桌面机操作系统中，执行相关的 DAM 策略，采集终端的软、硬件资产信息；监控一些敏感资产的变更；执行软件分发、外设管理任务。DAM 代理负责转发 iNode 客户端桌面服务器的交互报文。DAM 服务器负责向客户端下发桌面安全相关策略，接受客户端上报的相关信息，并存入数据库中。

DAM 功能分为资产管理、软件分发和外设管理 3 个部分。资产管理包括资产注册、资产查询、资产变更管理；软件分发包括 FTP 方式、HTTP 方式、文件共享方式；外设管理包括：U 盘的拔插、写入监控；禁用 USB、光驱、软驱、串口、并口、红外、蓝牙、1394、MODEM。

5.4 本章小结

华为终端安全管理系统以技术手段降低部署成本和复杂性，为内网终端安全管理提升效率并减轻压力。TSM 终端安全管理系统由终端安全管理服务器、安全接入控制设备和终端安全代理组成。其中，安全接入控制设备支持安全接入网关、802.1X 交换机、华为系列交换机、华为系列 AC/AP 设备和防火墙等设备。

H3C EAD 解决方案主要由 iNode 智能客户端、安全联动设备、iMC 服务器以及第三方服务器组成，是集成了网络准入、终端安全和桌面管理的内网安全解决方案。它可以和接入交换机、路由器、防火墙配合不影响网络性能，是网络准入控制和网络结构完美的结合！

第 6 章　信息安全工程原理

导入语：本章通过介绍信息安全工程的主要原理和最常见的 SSE-CMM 模型，使读者能够理解信息安全建设必须同信息化建设“同步规划、同步实施”的原则以及掌握如何运用信息安全能力成熟度模型理论评价和改进信息安全工程能力。

本章主要知识结构如图 6.1 所示。

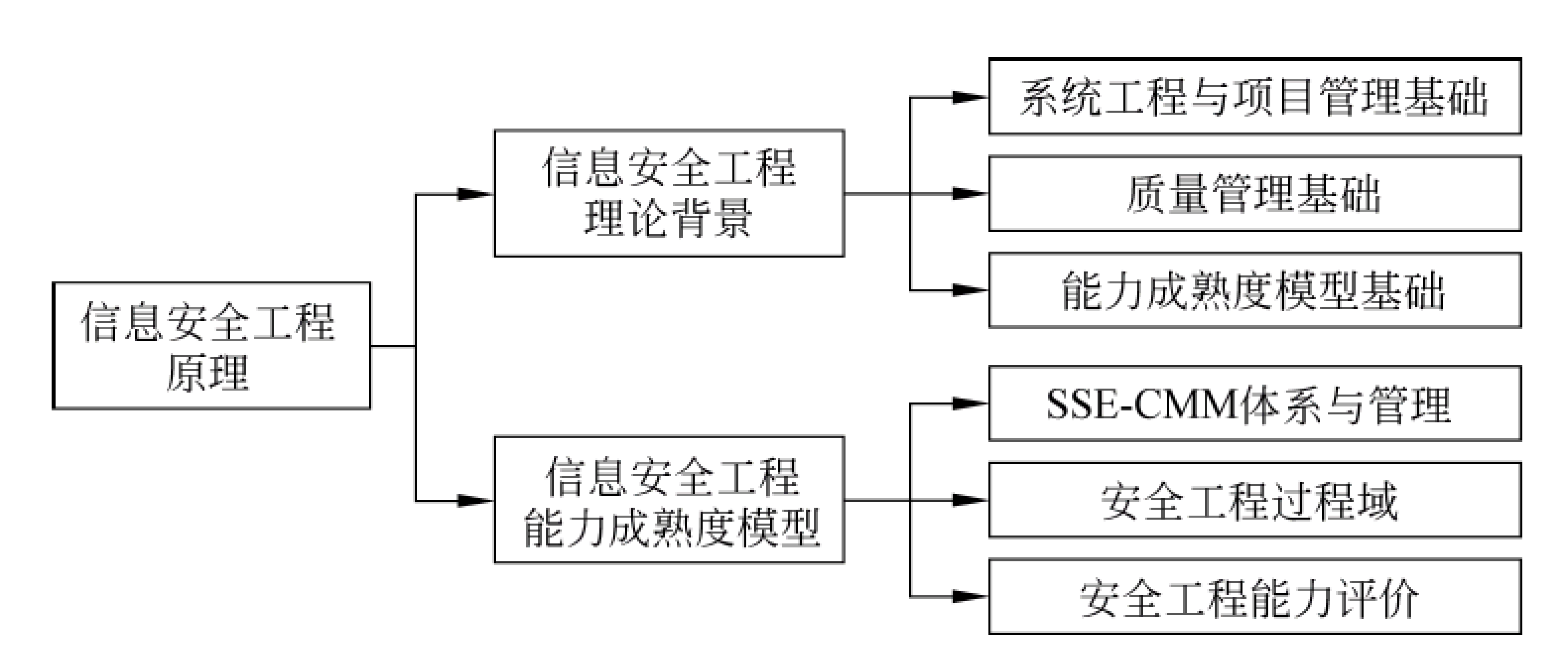


图 6.1　本章主要知识结构框图

安全工程理论背景部分，主要介绍了系统工程与项目管理基础、质量管理基础和能力成熟度模型基础，通过介绍这些知识，增强读者对相关知识的理解，为以后介绍的 SSE-CMM 模型奠定基础。

安全工程能力成熟度模型部分，详细介绍了 SSE-CMM 体系与管理的背景、发展历史、过程域，并举例说明如何利用该模型进行安全工程能力评价。

考核目标：安全工程理论背景部分要求读者能够理解系统工程与项目管理基础，包括了解系统工程基本思想和了解项目管理基本概念和要素；了解质量管理基本概念和 8 项质量管理基本原则；理解“工程能力成熟度”基本思想，了解能力成熟度模型的应用范围并能够指出“过程能力方案”和“组织机构成熟度方案”的区别。

安全工程能力成熟度模型部分要求读者能够了解 SSE-CMM 的适用范围，过程、过程区和过程能力的概念和域维/安全过程区与能力维/公共特征的关系；了解过程类、过程区和基本实施的关系，理解风险过程、工程过程和保证过程的含义和各个安全工程过程区的含义；理解能力级别、公共特征和通用实施的关系，理解各个信息安全工程能力级别的含义，并最终能够将相关的知识真正灵活运用到实际工程或项目中。

6.1　信息安全工程理论背景

6.1.1　系统工程与项目管理基础

首先看一个简单的例子。我国的《消防通道设计规范》中明确规定：“商住楼中住宅的疏散楼梯应独立设置”，如果在大楼的设计和实施阶段没有考虑消防，把楼盖完了，再去设置

消防通道，必然会导致成本的上升和安全性的下降。而安全工程在信息化建设中的重要性与其相比有过之而无不及。

同样地，在信息化建设中，假如A公司开展家用电话自助刷卡支付业务，用户可以通过其网站查询个人付款信息。第三方安全测评发现该网站存在SQL注入漏洞，可以泄露用户交易信息，但是当初外包开发此网站的公司已经倒闭，A公司技术人员对网站系统开发情况不了解，没有能力消除该漏洞。公司董事会研究最终决定，为保护用户隐私，只能暂时不再为用户提供网上交易信息查询服务。由此可见，如果项目在规划过程中就存在问题，那么无疑将会给之后的工作带来非常大的困难。

因此，安全工程的作用就日益突出。由于信息系统的建设是一项系统工程，具有复杂性，信息安全问题是信息系统与生俱来的，所以安全工程是以最优费效比提供并满足安全需求。值得注意的是，安全工程是信息化建设必要的有机组成部分，信息安全建设必须同信息化建设"同步规划、同步实施"，"重功能、轻安全"、"先建设、后安全"都是信息化建设的大忌。

信息安全工程可以参考的理论基础主要有系统工程思想、项目管理方法、质量管理体系和能力成熟度模型4项，本节主要讨论系统工程和项目管理。

1. 系统工程

首先，系统工程是一种方法论。我国著名科学家钱学森曾经对系统工程做过详细的定义："系统工程是组织管理系统规划、研究、制造、试验、使用的科学方法，是一种对所有系统都具有普遍意义的科学方法"。由此可见，系统工程不是基本理论，也不属于技术实现，而是一种方法论。

系统工程主要具有以下特点。

(1) 系统工程不同于一般的工程技术学科，如水利工程、机械工程等"硬"工程；系统工程偏重于工程的组织与经营管理一类"软"科学的研究。

(2) 系统工程涉及各种学科、各个领域的各种内容，因此它是跨越不同学科的综合性科学。

(3) 以整体的、综合的、关联的、科学的、实践的观点来看待研究对象。

(4) 在解决一个具体项目时，它要求把项目或过程分成几大步骤，而每个步骤又按一定的程序展开。这就保证了系统思想在每个部分、每个环节上体现出来。

(5) 任何系统都是人、设备和过程的有机组合，其中人是最主要的因素。因此在应用系统工程的方法处理系统问题时，要以人为中心。

霍尔三维结构集中体现了系统工程方法的系统化、综合化、最优化、程序化和标准化等特点，是系统工程方法论的重要基础内容。它将系统的整个管理过程分为前后紧密相连的6个阶段和7个步骤，并同时考虑到为完成这些阶段和步骤的工作所需的各种专业管理知识。三维结构由时间维、逻辑维、知识维组成，如图6.2所示。

运用SE知识，把三维结构中的6个时间阶段和7个逻辑步骤结合起来，便形成霍尔管理矩阵，如表6.1所示。

在霍尔管理矩阵中，时间维的每一阶段与逻辑维的每一步骤所对应的点a_{ij}代表着一项具体的管理活动。矩阵中的各项活动相互影响、紧密联系，要使整体上达到最优，必须使各阶段、步骤的活动反复进行。反复性是霍尔管理矩阵的一个重要特征，它反映了从规划到更换的过程需要控制、调节和决策。因此，系统工程充分体现了计划、组织和控制职能。

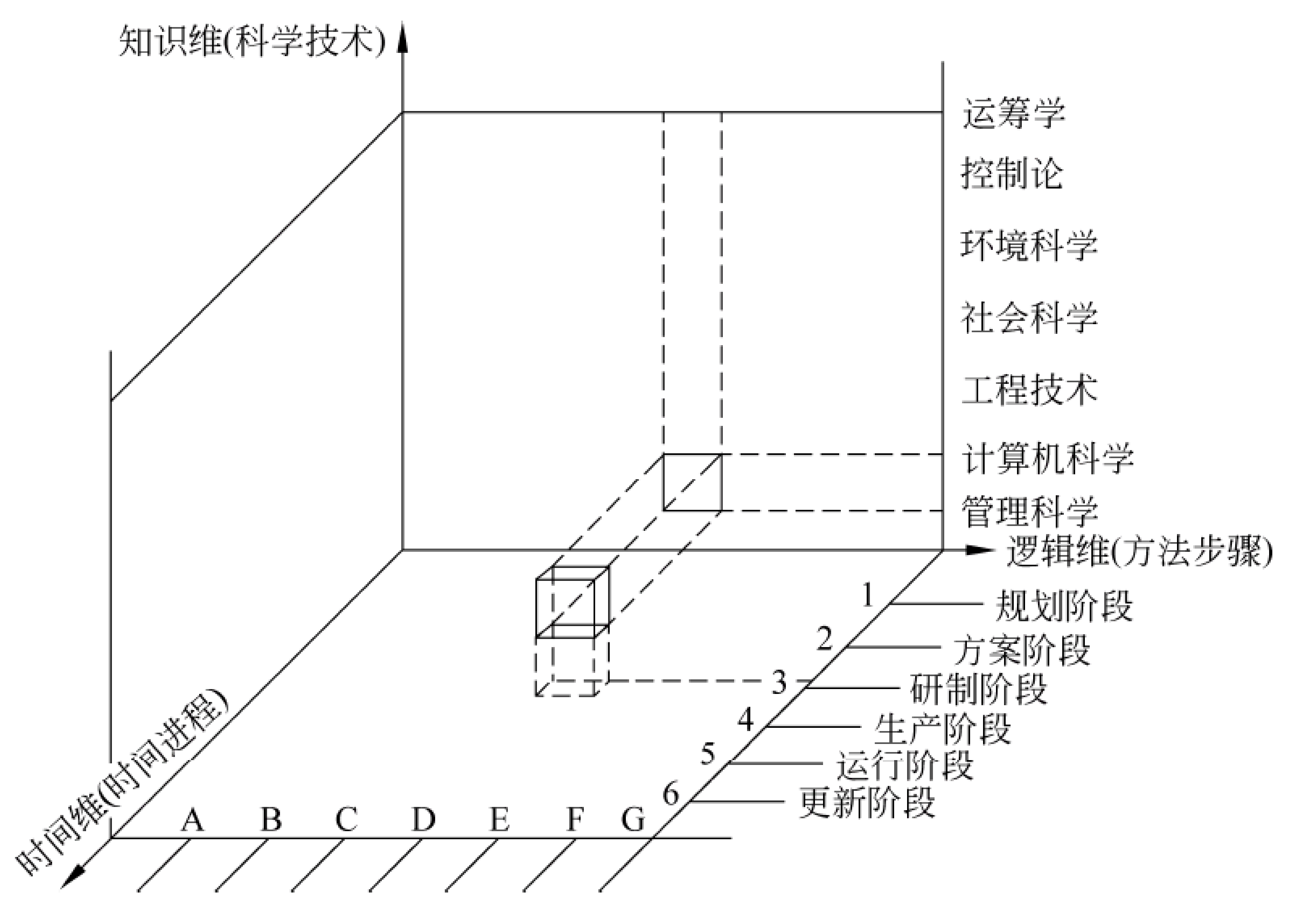


图 6.2　霍尔三维结构示意图

表 6.1　霍尔管理矩阵

逻辑维(步骤) / 时间维(阶段)	1 明确问题	2 选择目标	3 系统综合	4 系统分析	5 方案优化	6 作出决策	7 付诸实施
1. 规划阶段	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}
2. 方案阶段	a_{21}	a_{22}	a_{23}	a_{24}	a_{25}	a_{26}	a_{27}
3. 研制阶段	a_{31}	a_{32}	a_{33}	a_{34}	a_{35}	a_{36}	a_{37}
4. 生产阶段	a_{41}	a_{42}	a_{43}	a_{44}	a_{45}	a_{46}	a_{47}
5. 运行阶段	a_{51}	a_{52}	a_{53}	a_{54}	a_{55}	a_{56}	a_{57}
6. 更新阶段	a_{61}	a_{62}	a_{63}	a_{64}	a_{65}	a_{66}	a_{67}

霍尔管理矩阵可以提醒人们在哪个阶段该做哪一步工作,同时明确各项具体工作在全局中的地位和作用,从而使工作得到合理安排。

2. 项目管理

项目管理是指项目的管理者,在有限的资源约束下,运用系统的观点、方法和理论,对项目涉及的全部工作进行有效的管理。即从项目的投资决策开始到项目结束的全过程进行计划、组织、指挥、协调、控制和评价,以实现项目的目标。

项目管理的要素主要由以下几点组成。

(1) 项目范围管理。它是为了实现项目的目标,对项目的工作内容进行控制的管理过程。它包括范围的界定、范围的规划、范围的调整等。

(2) 项目时间管理。它是为了确保项目最终按时完成的一系列管理过程。它包括具体活动界定、活动顺序、时间估计、进度安排及时间控制等项工作。

(3) 项目成本管理。它是为了保证完成项目的实际成本、费用不超过预算成本、费用的管理过程。它包括资源的配置,成本、费用的预算以及费用的控制等项工作。

(4) 项目质量管理。它是为了确保项目达到客户所规定的质量要求所实施的一系列管

理过程。它包括质量规划、质量控制和质量保证等。

（5）人力资源管理。它是为了保证所有项目关系人的能力和积极性都得到最有效地发挥和利用所采取的一系列管理措施。它包括组织的规划、团队的建设、人员的选聘和项目的班子建设等一系列工作。

（6）项目沟通管理。它是为了确保项目的信息的合理收集和传输所需要实施的一系列措施。它包括沟通规划、信息传输和进度报告等。

（7）项目风险管理。涉及项目可能遇到各种不确定因素。它包括风险识别、风险量化、制订对策和风险控制等。

（8）项目采购管理。这是为了从项目实施组织之外获得所需资源或服务所采取的一系列管理措施。它包括采购计划、采购与征购、资源的选择以及合同的管理等项目工作。

（9）项目集成管理。这是指为确保项目各项工作能够有机地协调和配合所展开的综合性和全局性的项目管理工作和过程。它包括项目集成计划的制定、项目集成计划的实施、项目变动的总体控制等。

6.1.2 质量管理基础

要想了解质量管理，首先要知道什么是质量。

在质量管理体系 ISO 9000 中，质量被称为“一组固有特性满足要求的程度”；而 ISO 8402 则称其为“反映实体满足明确和隐含需要的能力的特性总合”。可以说，从不同的视角看，信息系统的质量可分为内部质量、外部质量和使用质量。

质量管理是指全部管理职能的一个方面。该管理职能负责质量方针的制订与实施。质量管理可以理解为为了实现质量目标而进行的所有管理性质的活动。在质量方面的指挥和控制活动，通常包括制定质量方针和质量目标以及质量策划、质量控制、质量保证和质量改进。

提到质量管理体系，不得不提到 ISO 9000 簇标准。

ISO 9000 簇标准并不是产品的技术标准，而是针对组织的管理结构、人员、技术能力、各项规章制度、技术文件和内部监督机制等一系列体现组织保证产品及服务质量的管理措施的标准。

ISO 9000 簇标准从以下 4 个方面规范质量管理。

（1）机构。标准明确规定了为保证产品质量而必须建立的管理机构及职责权限。

（2）程序。组织的产品生产必须制定规章制度、技术标准、质量手册、质量体系、操作检查程序，并使之文件化。

（3）过程。质量控制是对生产的全部过程加以控制，是面的控制，不是点的控制。从根据市场调研确定产品、设计产品、采购原材料，到生产、检验、包装和储运等，其全过程按程序要求控制质量。并要求过程具有标识性、监督性、可追溯性。

（4）总结。不断地总结、评价质量管理体系，不断地改进质量管理体系，使质量管理呈螺旋式上升。

6.1.3 能力成熟度模型基础

能力成熟度模型，也就是 CMM，这是对于软件组织在定义、实施、度量、控制和改善其

软件过程的实践中各个发展阶段的描述。CMM 的核心是把软件开发视为一个过程,并根据这一原则对软件开发和维护进行过程监控和研究,以使其更加科学化、标准化、使企业能够更好地实现商业目标。

CMM 是一种用于评价软件承包能力并帮助其改善软件质量的方法,侧重于软件开发过程的管理及工程能力的提高与评估。

CMM 为软件企业的过程能力提供了一个阶梯式的改进框架,它基于过去所有软件工程过程改进的成果,吸取了以往软件工程的经验教训,提供了一个基于过程改进的框架;它指明了一个软件组织在软件开发方面需要管理哪些主要工作、这些工作之间的关系以及以怎样的先后次序一步一步地做好这些工作而使软件组织走向成熟。

能力成熟度模型的基本思想是只要集中精力持续努力去建立有效的软件工程过程的基础结构,不断进行管理的实践和过程的改进,就可以克服软件生产中的困难。CMM 是目前国际上最流行、最实用的一种软件生产过程标准,已经得到了众多国家以及国际软件产业界的认可,成为当今企业从事规模软件生产不可缺少的一项内容。

在信息时代,软件质量的重要性越来越为人们所认识。软件是产品、是装备、是工具,其质量使得顾客满意,是产品市场开拓、事业得以发展的关键。而软件工程领域在 1992—1997 年取得了前所未有的进展,其成果超过软件工程领域过去 15 年来的成就总和。

20 世纪 70 年代中期,当时美国国防部曾立题专门研究软件项目做不好的原因,发现 70%的项目是因为管理不善而引起的,而并不是因为技术实力不够,进而得出一个结论,即管理是影响软件研发项目全局的因素,而技术只影响局部。

到了 20 世纪 90 年代中期,软件管理工程不善的问题仍然存在,大约只有 10%的项目能够在预定的费用和进度下交付。

导致软件项目失败的原因非常多,在关系到软件项目成功与否的众多因素中,软件度量、工作量估计、项目规划、进展控制、需求变化和风险管理等都是与工程管理直接相关的因素。由此可见,软件管理工程的意义至关重要。

1987 年,美国卡内基·梅隆大学软件研究所(SEI)受美国国防部的委托,率先在软件行业从软件过程能力的角度提出了软件过程成熟度模型(CMM),随后在全世界推广实施一种软件评估标准,用于评价软件承包能力并帮助其改善软件质量的方法。它主要用于软件开发过程和软件开发能力的评价和改进。它侧重于软件开发过程的管理及工程能力的提高与评估。CMM 自 1987 年开始实施认证,现已成为软件业最有权威的评估认证体系。CMM 包括 5 个等级,共计 18 个过程域,52 个目标,300 多个关键实践。

因为问题是由管理软件过程的方法引起的,所以新软件技术的运用不会自动提高生产率和利润率。CMM 有助于组织建立一个有规律的、成熟的软件过程。改进的过程将会生产出质量更好的软件,使更多的软件项目免受时间和费用的超支之苦。

软件过程的改善不可能在一夜之间完成,CMM 是以增量方式逐步引入变化的。CMM 明确地定义了 5 个不同的“成熟度”等级,一个组织可按一系列小的改良性步骤向更高的成熟度等级前进,如图 6.3 所示。

随着能力成熟度模型的发展,能力成熟度模型目前已经被广泛应用于各领域的工程过程改进,如图 6.4 所示。

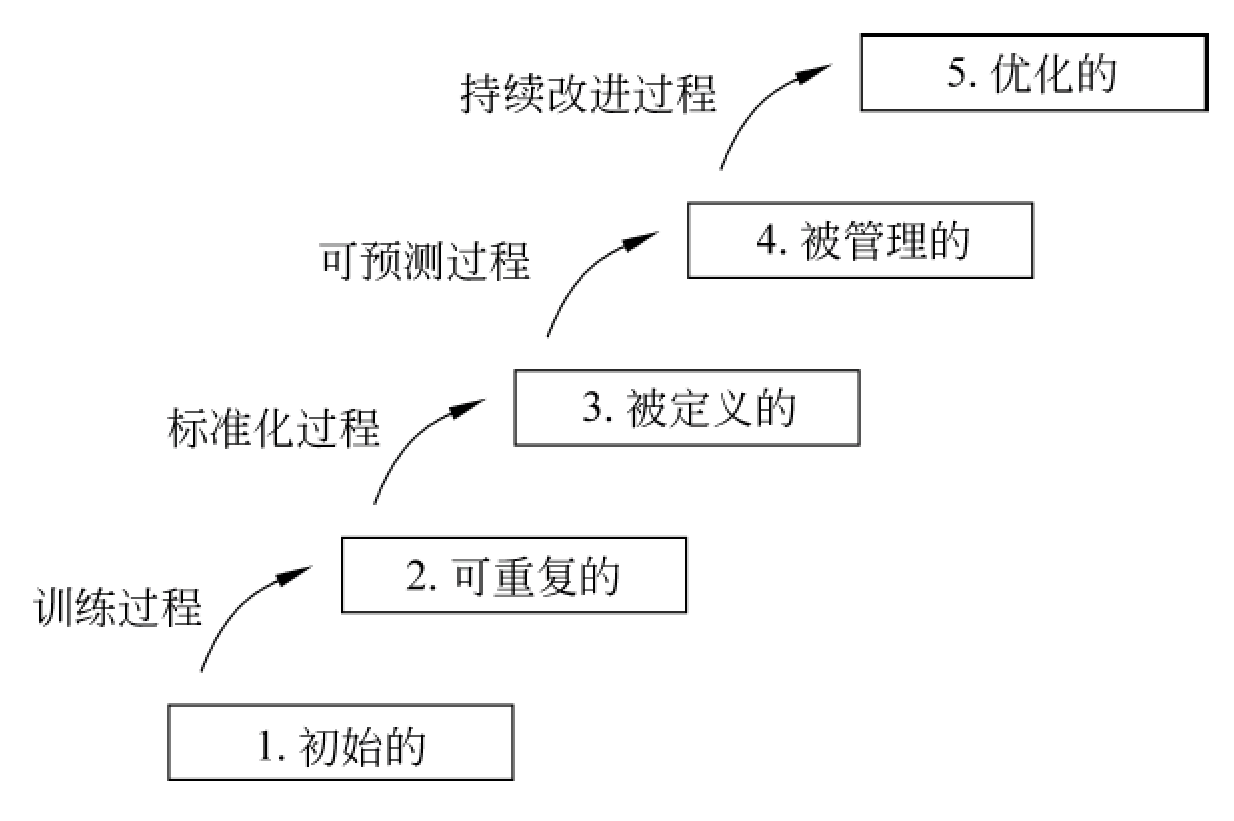


图 6.3　CMM 的 5 个"成熟度"等级

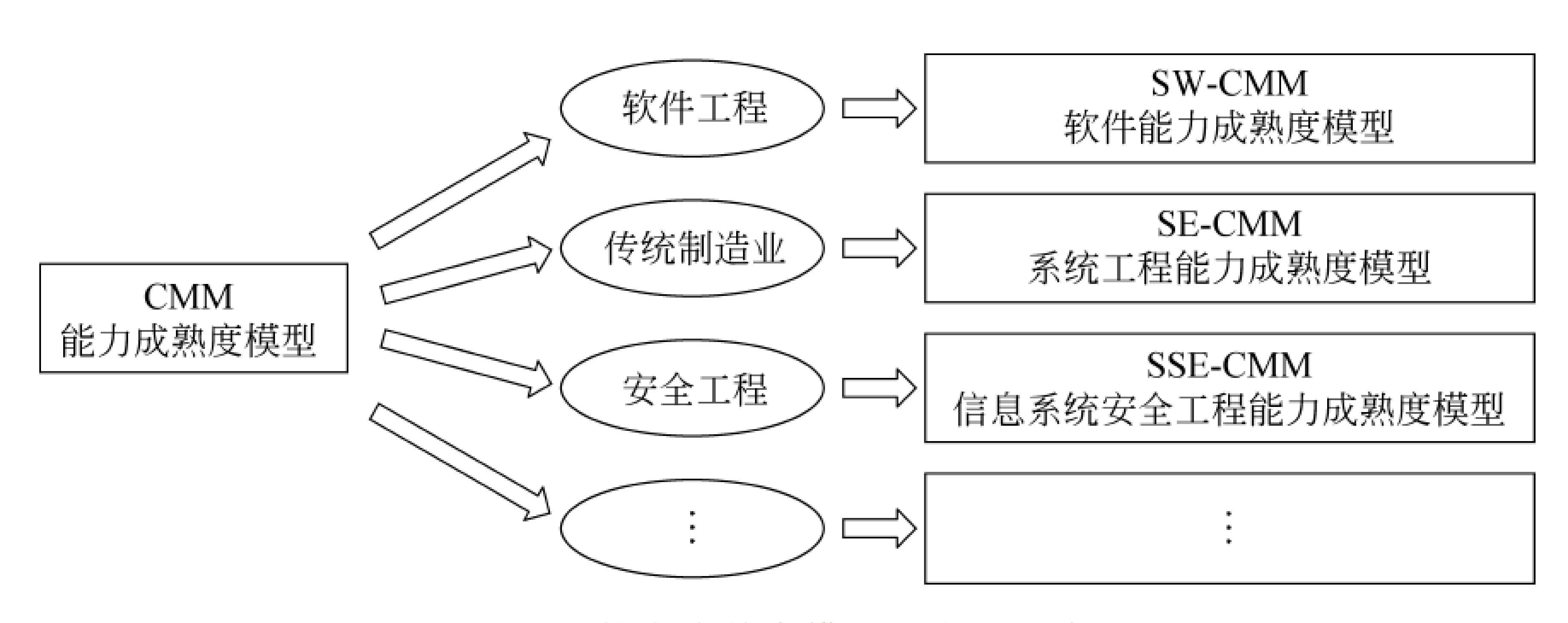


图 6.4　能力成熟度模型的发展和应用

6.2　信息安全工程能力成熟度模型

6.2.1　SSE-CMM 体系与原理

1. SSE-CMM 的基本概念

系统安全工程能力成熟度模型(Systems Security Engineering Capability Maturity Model,SSE-CMM)描述了一个组织的安全工程过程必须包含的基本特性,这些特性是完善安全工程的保证,也是信息安全工程实施的度量标准,同时还是一个易于理解的评估系统安全工程的框架。

SSE-CMM 是 CMM 在系统安全工程这个具体领域应用而产生的一个分支,主要用于评估实施者在信息安全建设过程中表现出来的能力和水平,可以为产品开发商改进安全产品、系统和服务的开发提供帮助,并为安全工程原则的应用提供了一个衡量和改进的途径。

SSE-CMM 对安全工程做了全方位刻画。

(1) 获取对企业中安全风险的理解。

(2) 获取安全需求。

(3) 将安全需求转换成安全指南。

(4) 在正确、有效的安全机制下建立信心和保证。

(5) 判断系统中是否存在可接受的风险。

(6) 将所有工程过程和专业活动融合为一个对系统安全可信的综合理解。

2. SSE-CMM 的宗旨和目标

SSE-CMM 的宗旨是为在信息安全建设中需要提供一个清晰定义的、成熟的且可测量的要求。

SSE-CMM 的目标主要有 3 点：通过区分投标者的能力级别和相关的计划风险来选择合格的安全工程提供商；有利于工程组把投资集中在安全工程工具、培训、过程定义、管理实施和改进上；提供基于能力的保障，也就是说，用户可以基于对工程组安全工程实践和过程的成熟度而确保信心。

3. SSE-CMM 的发展历史

作为一个成熟的模型，SSE-CMM 也经历了一段漫长的发展过程。表 6.2 给出了 SSE-CMM 的发展历程，以便读者能够更详细地了解 SSE-CMM。

表 6.2　SSE-CMM 发展历程

时　　间	发　　展
1993 年 4 月至 1994 年 12 月	预研究(NSA)
1995 年 1 月	第一次公共会议，工作组成立
1995 年 3 月	第一次工作组会议
1996 年秋	进行 SSE-CMM 实验项目
1996 年 10 月	发布 SSE-CMM v1.0
1997 年春	发布评定方法 v1.0
1997 年夏	发布 SSE-CMM v1.1 和评定方法 v1.1
1997 年 7 月	第二次公共会议
1999 年 4 月	发布 SSE-CMM v2.0，评定方法 v2.0
2002 年 3 月	被 ISO 接受为 ISO/IEC 21827
2003 年 6 月	发布 SSE-CMM v3.0

4. SSE-CMM 的适用对象

SSE-CMM 的适用对象，主要有以下 3 类。

(1) 工程组织(Engineering Organization)。

这一类主要包括系统集成商、应用开发商、产品提供商、服务提供商等，主要是利用 SSE-CMM 对自己的工程能力进行自我评估。

(2) 获取组织(Acquiring Organization)。

这一类主要包括采购系统、产品以及从外部或内部资源和最终用户处获取服务的组织，主要是利用 SSE-CMM 判别一个供应者组织的系统安全工程能力，识别该组织供应的产品和系统的可信任性。

(3) 评估组织(Evaluation Organization)。

这一类主要包括认证组织、系统授权组织和产品评估组织，主要是利用 SSE-CMM 作为工作基础，以便建立被评估组织整体能力的信任度，该信任度是系统和产品的安全保证

要素。

6.2.2　安全工程过程区域

1. 一些基本概念

(1) 过程(Process),是指为了达到某一给定目标而执行的一系列活动,这些活动可以重复、递归和并发地执行。

(2) 过程域(Process Area,PA),是由一些基本实施(Base Practices,BP)组成,这些 BP 共同实施以达到 PA 的目标。

SSE-CMM 包含 3 类过程域：工程、项目和组织。

工作产品(Work Product),包括执行任何过程时产生的所有文档、报告、文件和数据。

过程能力(Process Capability),是通过跟踪一个过程能达到预期结果的可量化范围组织的过程能力可帮助组织预见项目达到目标的能力。

SSE-CMM 并不定义各过程域在系统安全工程生命周期中出现的顺序。过程域实际上是依照过程域名的英文字母顺序来编号的。每个过程域包括一组集成的 BP。BP 定义了实现过程域目标的必要活动,代表业界的最佳惯例。每个 BP 都规定了工作产品。

2. SSE-CMM 的 3 个基本过程域组

SSE-CMM 将安全工程划分为 3 类基本的过程域组：风险、工程和保证。

风险过程识别出所开发的产品或系统的危险性,并对这些危险性进行优先级排序。针对危险性所面临的问题,安全工程过程要与其他工程一起来确定和实施解决方案。最后,由安全保证过程来建立对解决方案的信任并向顾客转达这种安全信任。三者之间的关系大致可以由图 6.5 表示。

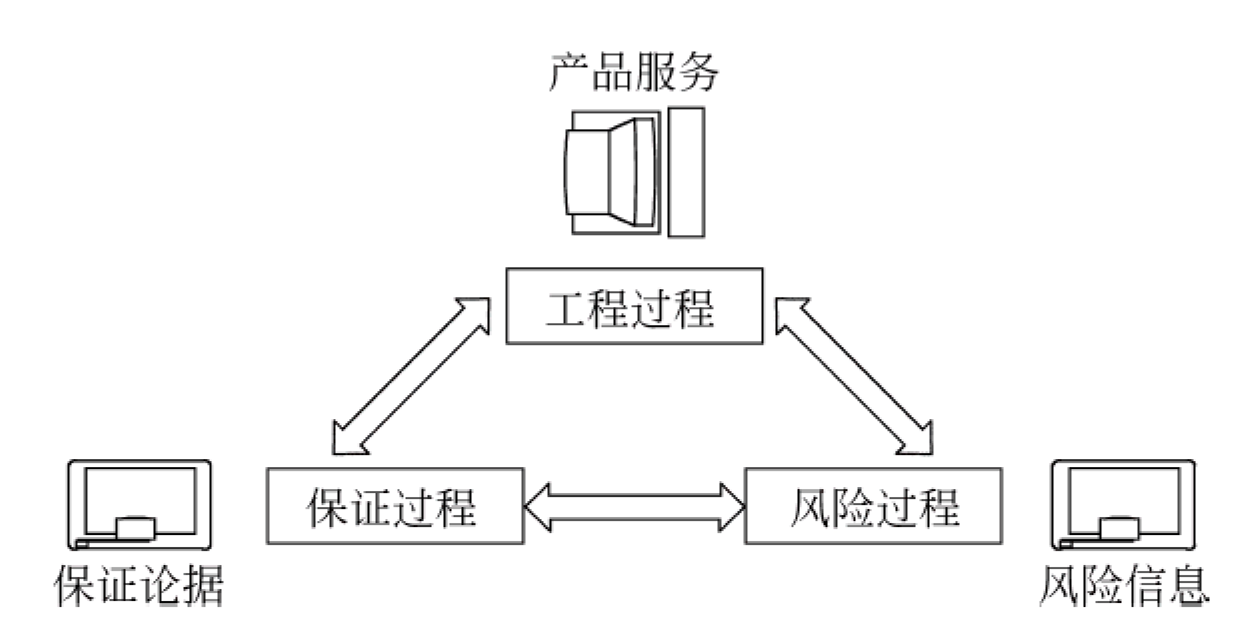


图 6.5　SSE-CMM 三类过程域之间的关系

1) 风险过程

一般来说,一个有害事件由 3 个部分组成：威胁、脆弱性和影响。如果不存在脆弱性和威胁,就不存在有害事件,也就不存在风险。

安全措施的实施可以减轻风险。安全措施可针对威胁、脆弱性、影响和风险自身。但无论如何,并不能消除所有威胁或根除某个具体威胁。这主要是因为风险消除的代价和相关的不确定性。因此,必须接受残留的风险。在存在很高的不确定性的情况下,由于风险的不精确的本质,因此是否接受风险是需要慎重对待的大问题。

SSE-CMM 过程域包括威胁、脆弱性、影响和相关风险进行分析的活动保证。

风险过程有 4 个过程域：PA02 评估影响、PA03 评估安全风险、PA04 评估威胁、PA05

评估脆弱性。其中 PA03 评估安全风险要在其他 3 个域进行完以后；而其他 3 个域则无严格时间顺序，如图 6.6 所示。

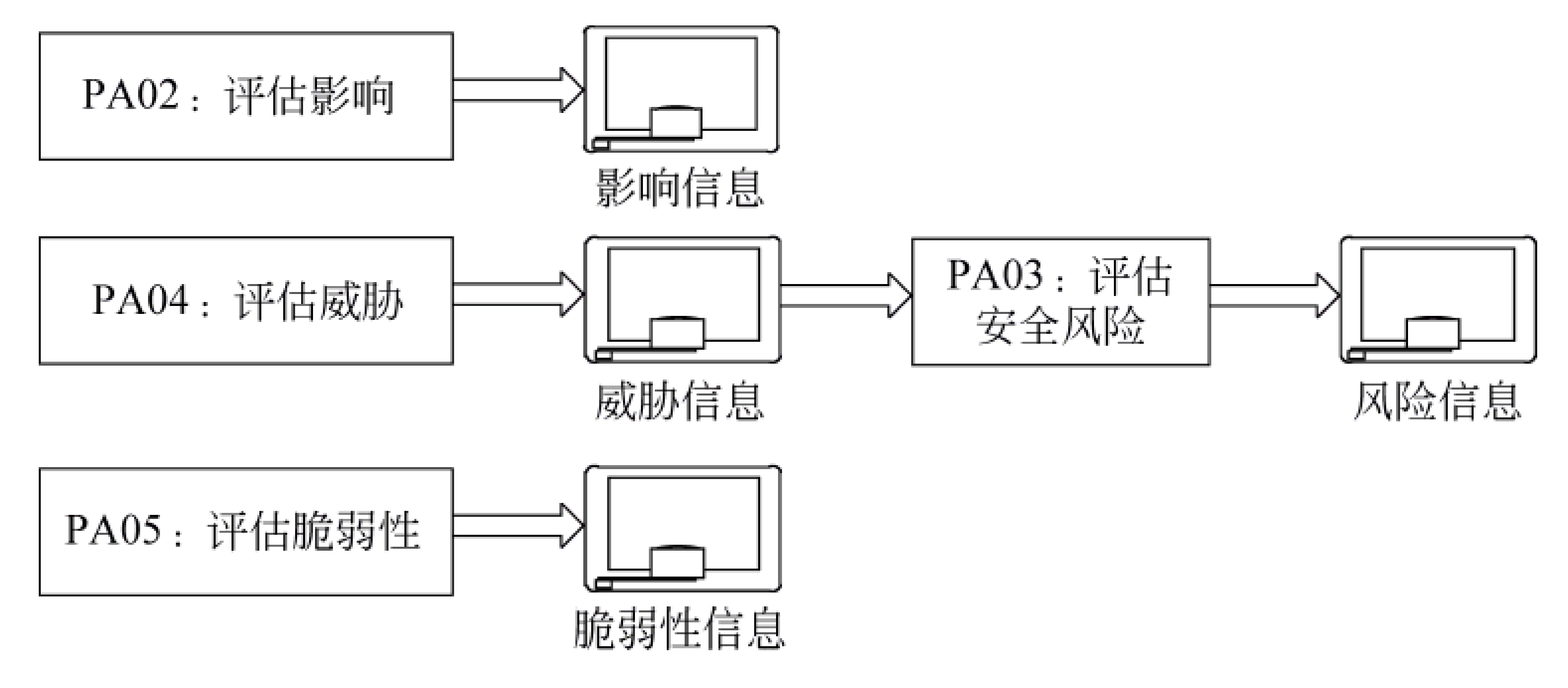


图 6.6　风险过程的 4 个过程域

PA02：评估影响。

该过程域的主要作用是识别和描述安全事件造成的影响。包括：识别系统中的资产；选择用于评估影响的度量标准；识别潜在的影响，列出描述影响的清单；对影响进行分析和优先级排序；监控影响中发生的变化。

PA03：评估安全风险。

该过程域的主要作用是识别和描述系统面临的安全风险。包括：选择风险分析的方法、技术和标准；识别威胁/脆弱性/影响的三组合(暴露)；评估与每个暴露有关的风险；对风险进行优先级排序及创建安全措施需求清单；监控风险的变化。

PA04：评估威胁。

该过程域的主要作用是识别和描述系统面临的安全威胁及其特征。包括：识别自然因素所引起的有关威胁；识别人为因素所引起的有关威胁；制定评判威胁的测度单位，即用什么指标来衡量威胁的高低；评估威胁源的动机和能力，即攻击者对系统有多大兴趣，攻击者拥有的知识、技能、工具和其他资源；评估威胁事件出现的可能性；监控威胁的变化。

PA05：评估脆弱性。

该过程域的主要作用是识别和描述系统存在的脆弱性及其特征。包括：选择识别和描述系统脆弱性的方法、技术和标准；识别系统中存在的脆弱性；收集与脆弱性特征有关的数据；对脆弱性进行综合分析，评判脆弱性或脆弱性组合可能带来的危害；监控脆弱性的变化。

2）工程过程

工程过程是一个以 PA07 协调安全为核心的，时间上的循环过程，就其每个过程域的实现而言，是有时间顺序的。可以与 PDCA 信息安全管理过程类比映射。

在这个过程中，安全工程的实施必须紧密地与其他的系统工程队伍合作。SSE-CMM 强调安全工程师是一个大的项目队伍中的一部分，需要与其他科目工程师的活动相互协调。这会有助于保证安全成为一个大的项目过程中一个整体部分，而不是一个分开的独立活动。

对于安全问题，创建安全解决方案一般包括识别可能选择的方案，然后评价决定哪一种更可以被接受。将这个活动与后面工程活动相结合的困难是解决方案不能只考虑安全问题。而是需要考虑其他因素，其中包括成本、性能、技术风险、是否容易使用。这些决定应加以收集以尽可能减少不断重复涉及这些问题。这些得到的分析也构成对安全保证结果的重

要基础。

在生命周期的后面阶段，安全工程师将根据意识到的风险来适当地配置系统，以确保新的风险不会造成系统运行的不安全状态。

工程过程有 5 个过程域：PA01 实施安全控制、PA07 协调安全、PA08 监视安全态势、PA09 提供安全输入、PA10 确定安全需求，如图 6.7 所示。

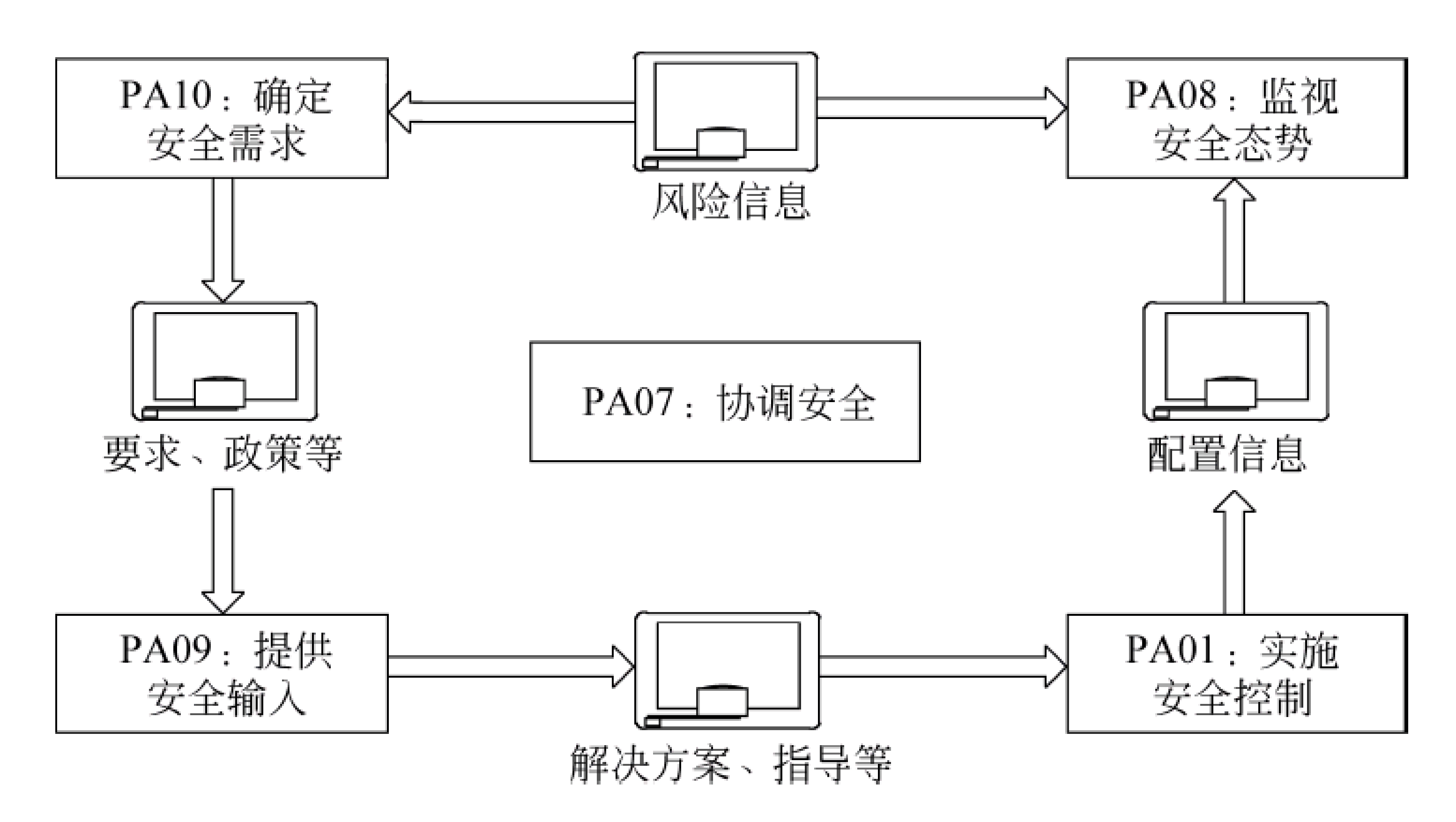


图 6.7　工程过程的 5 个过程域

PA01：实施安全控制。

该过程域的主要作用是确定集成到系统中的安全控制措施确实在系统运行过程中发挥预计的安全功能。包括：建立安全控制措施的责任，落实有关责任人；对系统安全控制的配置进行管理；对系统用户和管理员进行安全意识教育和技能培训；对安全服务和控制机制进行定期维护，避免损伤和故障。

PA07：协调安全。

该过程域的主要作用是保证所有部门都有一种参与安全工程的意识。包括：确定各部门的职责和关系；确定安全工程中的协调机制；制定解决冲突的方法，促进协调机制的落实；使各部门、各工程实施组了解和接受有关安全的决定和建议。

PA08：监视安全态势。

该过程域的主要作用是及时发现安全措施状态变化及安全事件，并进行适当的处置。包括：监控威胁、脆弱性、影响等方面的变化；分析安全态势，及时发现需要加强或调整的安全措施；监控安全防护措施的功能、性能的有效性；及时发现安全突发事件，并作出及时有效的响应；分析事件记录，确定事件原因，总结避免再次发生的方法；保护安全监控得到的记录数据。

PA09：提供安全输入。

该过程域的主要作用是为系统的规划者、设计者、实施者和用户提供他们所需的安全信息（包括安全架构、安全设计、实施方法和安全指南等），即告诉“其他人”怎么做才能保证系统的安全。包括：分析论证系统建设方案的安全性；制定安全解决方案；为参与系统建设的非安全专业人员提供安全实施指南；为系统用户和管理员提供安全运行指南。

PA10：确定安全需求。

该过程域的主要作用是根据系统的安全风险，以及政策法规的约束确定系统与安全相关的需求。包括：理解系统的用途，判断其安全需求的特点；理解系统用户的安全需求；识别政

策法规和其他约束(如合同)提出的安全需求;确定安全需求,包括信息安全的总体目标、系统开发和维护中应当实现的安全目标;相关方对安全需求达成一致,并获得系统用户的认可。

3) 保证过程

安全保证通常以安全论据的形式出现。安全论据包括一组对系统性质的要求。这些要求都要有证据来支持。证据在安全工程活动的正常过程期间获得并常常记录在文档中。

SSE-CMM 活动本身涉及与安全相关证据的产生。例如,过程文件能够表示开发是遵循一个充分定义的、成熟工程过程,这个过程需加以连续改进。安全验证和证实在建立一个可信产品或系统中起到主要作用。

回顾 ISSE 中的“有效性评估”以及 DOD5200.2-R 中的需求环、设计环概念,不难发现此处的“保证”含义在于在每个过程域的实施中保留充分的证据,提供对“已经正确实施控制”的证明,从而给客户以信心。

保证过程有两个过程域:PA06 建立保证论据和 PA11 验证和确认安全,如图 6.8 所示。

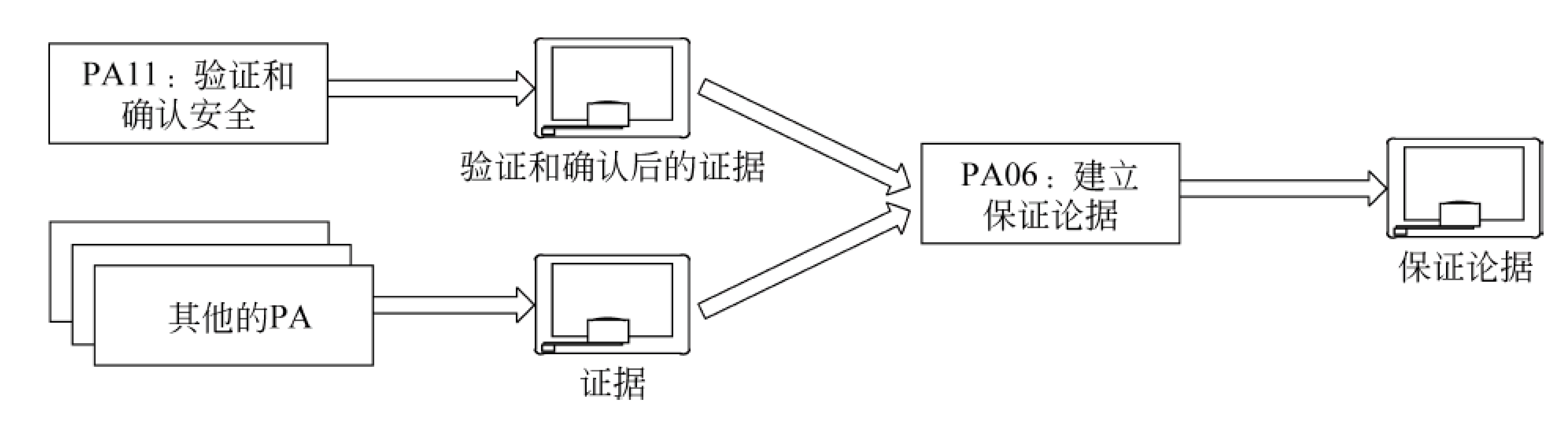


图 6.8 保证过程的两个过程域

PA06:建立保证论据。

该过程域的主要作用是清楚地说明用户的安全需求已经得到满足,通过一系列证据建立对系统安全的信心。包括:确定用户的安全保证目标,明确系统的安全需求等级(如等保定级);收集分析安全保证证据(如等保测试记录);提供安全保证证据(如等保测评报告)。

PA11:验证和确认安全。

该过程域的主要作用是通过观察、论证、分析和测试来验证和证实解决方案满足安全需求;验证证明正确性,证实证明有效性。包括:制定验证和证实目标和计划;制定验证和证实具体方法;实施验证和证实发现有关问题;提供验证和证实结果。

3. SSE-CMM 的基本模型

SSE-CMM 体系结构的设计目标是清晰地从管理和制度化特征中分离出安全工程的基本特征。为了保证这种分离,SSE-CMM 模型是两维的,分别称为“域”和“能力”。

域维主要汇集了定义安全工程的所有实践活动——基本实施(BP)。

能力维则代表了组织能力,由过程管理和制度化能力构成,即一系列通用实施(GP)过程。通用实施表现了一个基本实施中应当完成的活动。

图 6.9 给出了一个二维的 SSE-CMM 模型。由于安全工程的基础部分是识别安全脆弱性,该活动在 SSE-

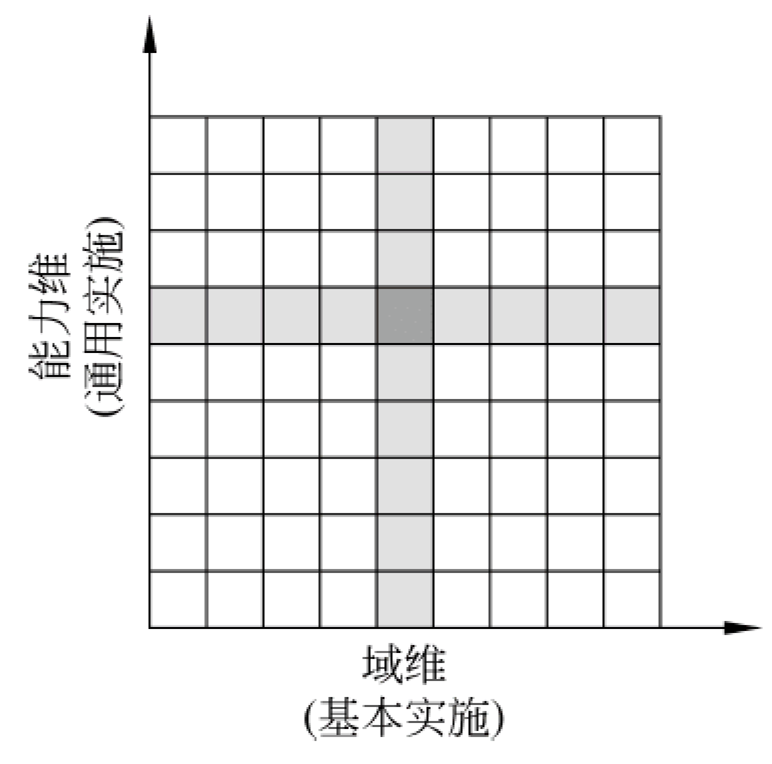


图 6.9 二维的 SSE-CMM 模型

CMM 中归于基本实施 05.02“识别系统安全脆弱性”，而确定一个组织是否有能力完成某项活动的方法之一，就是检查它是否有为声明要做的活动配置资源的过程。成熟组织具备的该“特征”，在 SSE-CMM 通用实施 2.1.1 中称为“配置资源”。

将基本实施和通用实施综合起来，为检查组织完成特定活动的能力提供了一种方法。例如，有意的一方可能问：“你们组织为识别系统安全脆弱性配置了资源吗?”得到的答案便是对组织能力的初步了解。回答全部基本实施和通用实施相结合而提出的所有问题(交叉点)，就能得到该组织安全工程能力的概貌。

在 SSE-CMM 中，SSE-CMM 域维包含了 61 个基本实施，这 61 个基本实施被归为了 11 个过程域(PA)，它们涵盖了所有主要的安全工程域。这些基本实施来自于广泛的材料、实践和专家知识。此外，SSE-CMM 中还定义了 11 个项目和组织过程域，这些过程域不是与安全直接相关的，但是它们也会对安全造成影响。

4. 基本实施和过程域的关系

基本实施和过程域之间的关系，可以大致用图 6.10 表示。

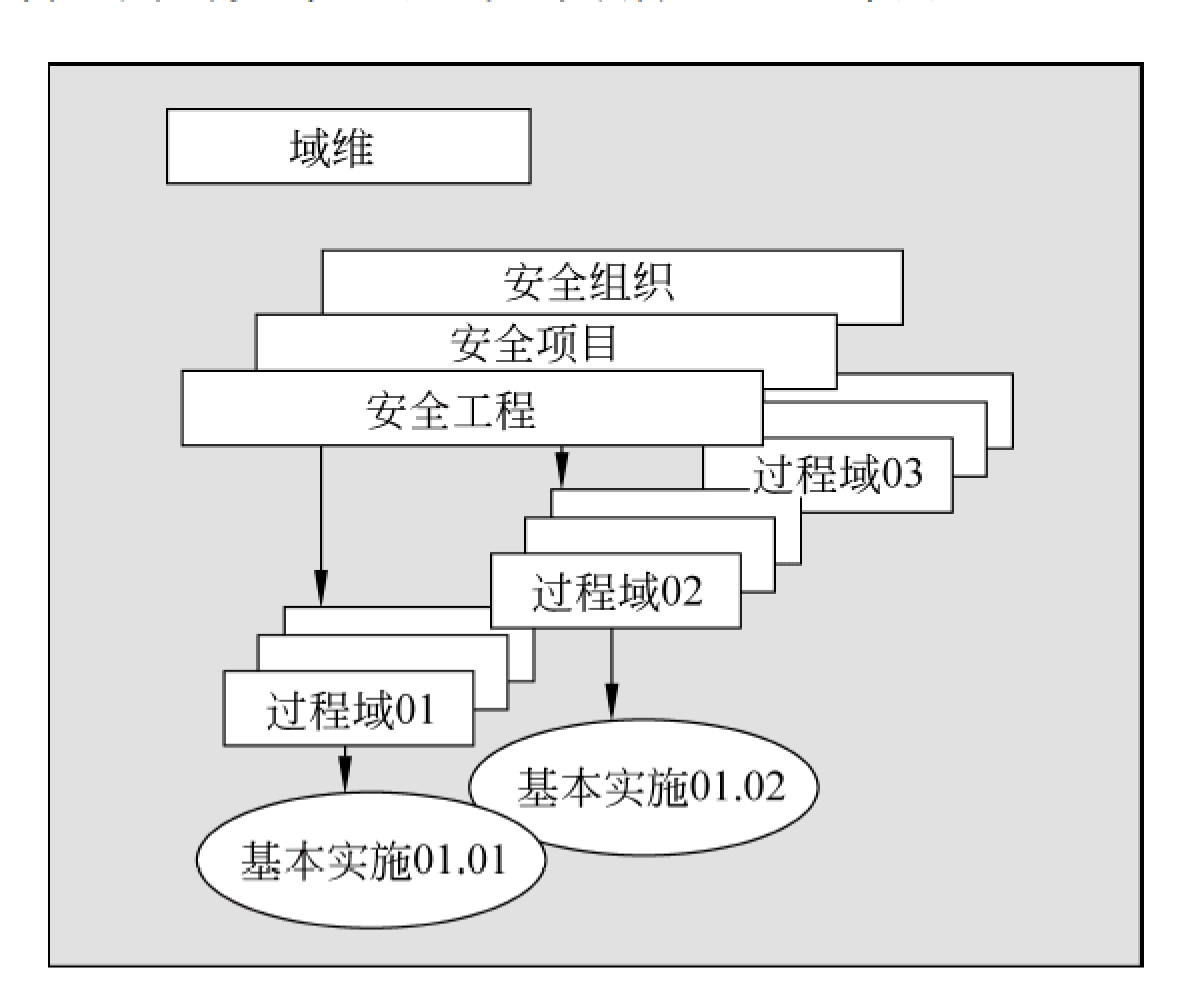


图 6.10　基本实施和过程域之间的关系

过程域的描述格式通常如下。

PA01——过程域名

概述——对该过程域的概括介绍

目标——实施该过程域期望达到的目标

基本实施列表——说明每一个基本过程的序号和名称

过程域注解——对该过程域的其他说明

BP.01.01——基本实施名

描述性名字——对该基本实施的一句描述

描述——对该基本实施的概括

工作成果示例——列出了所有可能的输出

注解——关于该基本实施的任何其他的注解

BP.01.02

例如，对过程域 PA05 的描述如下。

PA05——评估脆弱性

概述——评估安全脆弱性的目的在于标识和描述系统的安全脆弱性。本过程域包括分析系统资产、定义具体的脆弱性以及对整个系统的脆弱性进行评估。

目标——获得对一给定环境中系统安全脆弱性的理解。

基本实施清单：

BP05.01——选择脆弱性评估方法

描述——基本实施包括定义系统的脆弱性分析方法，以对安全脆弱性进行标识和描述……

工作结果示例：

脆弱性分析方法——讨论系统安全脆弱性的分析方法。

脆弱性分析格式——描述脆弱性分析结果的格式。

攻击方法学及其原理——实施攻击测试的目标和方法。

攻击过程——实施攻击测试的详细步骤。

攻击计划——资源、时间进度和攻击方法描述。

渗透研究——为标识已知或未知的脆弱性而采取的攻击方法和实施概要。

攻击概要——描述将要实施的具体攻击。

BP05.02——标识系统安全脆弱性

……

BP05.03——收集与脆弱性属性有关的数据

……

BP05.04——评估系统脆弱性

……

BP05.05——监视脆弱性及其特征的变化

……

过程域注解

……

5. 通用实施、公共特征与能力级别

SSE-CMM 能力维由通用实施(GP)构成。GP 是应用在所有过程中的行为。它们针对的是一个过程的管理、测量和制度化。与 BP 不同，通用实施的顺序根据成熟度排列。在通用实施维中，越向上表示成熟度级别越高。通用实施被归为若干类逻辑域，称为“公共特征”。若干个公共特征构成了 SSE-CMM 的能力级别。能力级别分为 5 级，5 级的要求则由这些公共特征所组成。

通用实施、公共特征与能力级别的关系如图 6.11 所示。

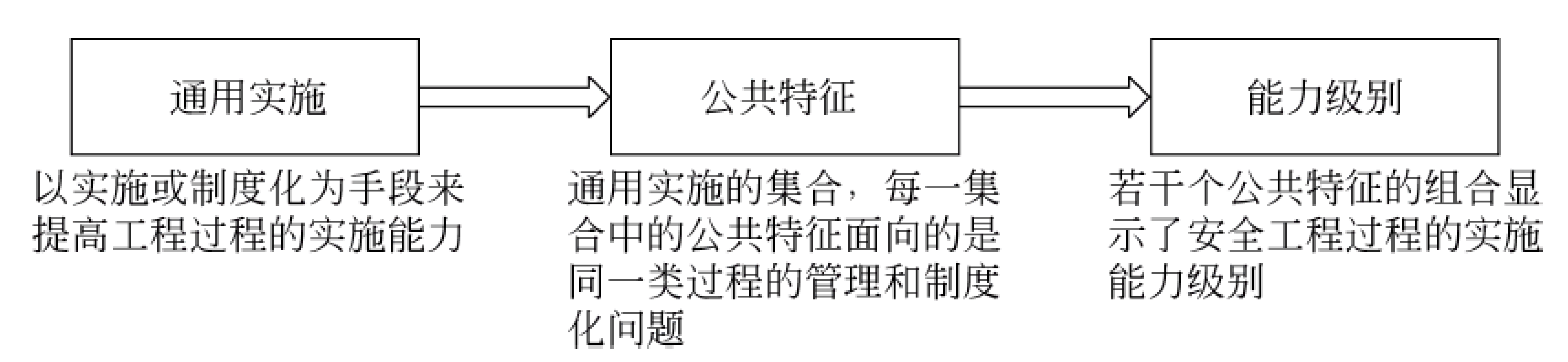


图 6.11　通用实施、公共特征与能力级别的关系

5 个能力级别及其包含的公共特征如图 6.12 所示。

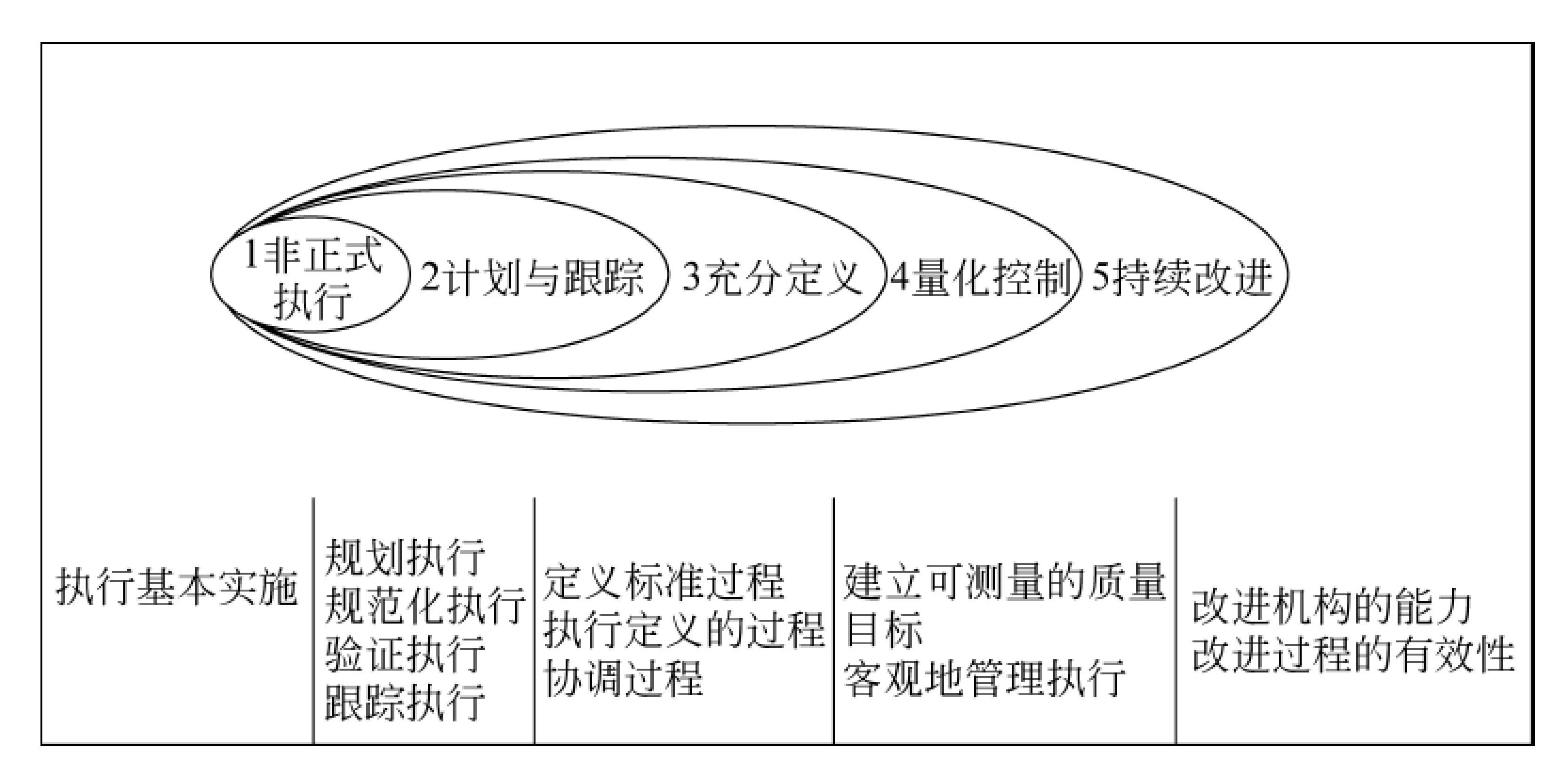


图 6.12　5 个能力级别及其包含的公共特征

(1) 非正式执行。

该级将关注一个机构或项目是否执行了包含基本实施过程的安全工程。该级别的特点可以描述为“你必须首先做它,然后才能管理它”。

在本级别,过程域中的基本实施通常已得到了执行。但这些基本实施的执行可能未经过严格的计划和跟踪,而是基于个人的知识和努力。

(2) 计划与跟踪。

该级将关注项目层面的定义、规划和执行问题。该级别的特点可描述为“在定义机构层面的过程之前,先要理解项目的相关事项”。

在本级别,基本实施的执行要经过规划并被跟踪。执行时要依据具体的流程,并应得到验证。工作结果要符合特定的标准和需求。执行情况还要经过测量,以使机构能够基于这些执行而管理其活动。它与非正式执行级的主要区别是过程的实施要经过规划和管理。

(3) 充分定义。

该级将关注于在机构层面上从既定过程中实施已融合了各个专业领域知识的裁剪结果。该级别的特点可描述为“用项目中学到的最好的东西来创建机构层面的过程”。

在本级别,基本实施应按照充分定义的过程来执行,执行过程中将使用已获批准的、经裁剪的标准。本级与第 2 级“计划与跟踪级”的主要区别在于本级将利用机构范围内的标准化过程来规划和管理安全工程过程。

(4) 量化控制。

该级将关注于测量,它是与机构的业务目标紧密联系在一起的。这个级别的特点可以描述为“只有你知道它是什么,你才能测量它”以及“当你测量正确的对象时,基于测量的管理才有意义”。

对过程执行情况的详细测量将在本级中进行收集和分析。这将形成对过程能力的量化理解,使机构有能力去预测过程的执行。

在本级别,过程执行的管理是客观的,工作结果的质量是量化的。本级与充分定义级的主要区别在于所定义的过程是可量化理解和控制的。

(5) 持续改进。

该级将从此前各级的所有管理活动中获得最大的收益,并强调机构的文化,以保持所取

得的成果。该级别的特点可以描述为"一个持续改进的文化需要以良好的管理措施、既定过程和可测量的目标为基础"。

在本级别,有关工程过程效果和效率的量化执行目标已经基于机构的业务目标而建立。过程的执行以及试验性的新概念和新技术产生了量化反馈,从而使基于这些目标的连续的过程改进得到了实现。本级与量化控制级的主要区别在于,在本级中,基于对这些过程变化效果的量化理解,工程中既定过程和标准过程将得到不断的改进和提高。

能力级别的描述格式通常如下。

能力级别 1——能力级别名

概述——对该级别能力的概括介绍

公共特征列表——说明每一个公共特征的序号和名称

公共特征 1.1——公共特征名

概述——对该公共特征的概括介绍

通用实施列表——说明每一个公共特征的序号和名称

GP1.1.1——通用实施名

描述——对该通用实施的概括介绍

注解——关于该通用实施的其他说明

关系——与 SSE-CMM 其他部分(如某些过程域)的关系

GP1.1.2……

例如,对能力级别 2 的描述如下。

能力级别 2——计划与跟踪

概述——在本级别上,基本实施的执行要经过规划并被跟踪。……

公共特征清单——该能力级别包含以下公共特征:

公共特征 2.1——规划执行

概述——本公共特征中的通用实施的重点在于对基本过程的实施进行规划。……

通用实施清单——该公共特征包含以下通用实施:

GP2.1.1——分配资源

描述——为过程域的执行提供充分的资源(包括人)。

注解

……

关系——关键资源的标识在过程域 PA16"规划技术活动"中进行。

GP2.1.2——分配责任

GP2.1.3——文档化过程

GP2.1.4——提供工具

GP2.1.5——确保培训

GP2.1.6——规划过程

……

公共特征 2.2——规范化执行

公共特征 2.3——验证执行

公共特征 2.4——跟踪执行

……

6.2.3　安全工程能力评价

通过以上几节的介绍，相信读者已经能够熟悉 SSE-CMM 的流程和操作方式，接下来本书将从应用的角度介绍 SSE-CMM 模型是如何对一个安全工程进行能力评价的。

1. 理解 SSE-CMM 应用

SSE-CMM 为每个能力级别定义了一个或多个公共特征。只有在所有这些公共特征都得到满足时，过程才达到了对应的能力级别。

工程组织可以根据系统安全工程项目的实际需求有选择地执行某些过程域而不是全部过程域。

工程组织应当针对每个过程域为自己评级，各过程域上的能力级别可能不同，这为工程组织过程能力的改善提供了方向。

一个常见的 SSE-CMM 的能力评价工作方式如下：

(1) 选择一个适合机构业务或任务的一个过程域。

(2) 查看该过程域的描述、目标及所包含的 BP。

(3) 查看机构中是否有在执行该过程域包含的所有 BP。

(4) 查看该过程域的目标是否得到了满足。

(5) 在相应的公共特征 1.1 处上做标记。

(6) 查看公共特征 2.1 中的描述和所包含的 GP。

(7) 对照公共特征 2.1 中的 GP，查看机构是否正在计划执行所选择的过程域。

(8) 如果步骤(7)得到满足，在公共特征 2.1 处做上标记，如未满足，则跳至步骤(10)。

(9) 对照第二级中的其他每一个公共特征，分别重复步骤(6)～(8)。

(10) 对每一个过程域，重复步骤(2)～(9)。

2. SSE-CMM 的应用场合

SSE-CMM 通常可用在 3 个方面：过程改进、能力评估和保证。

过程改进：可以使一个安全工程组织对其安全工程能力的水平有一个认识，以便设计经改进的安全工程过程，提高其安全工程过程能力。

能力评估：允许一个客户组织了解其提供商的安全工程过程能力。

保证：凭借证据对所采用工程的成熟度做出支持性声明，提高了产品、系统和服务的可信性。

3. IDEAL 模型

IDEAL 模型代表了过程改进活动的一个生命周期，它作为一个基础性的策略，已经在 SEI 的许多服务中采用。IDEAL 模型是用过程改进的 5 个阶段描述来命名的：初始化；诊断；建立；行动；学习。IDEAL 模型如图 6.13 所示。

(1) Initiating(初始化)。该阶段主要工作为熟悉项目目标和完成方式，开发业务案例和项目执行方法，获得管理层批准和支持，为成功的改进努力做好铺垫。

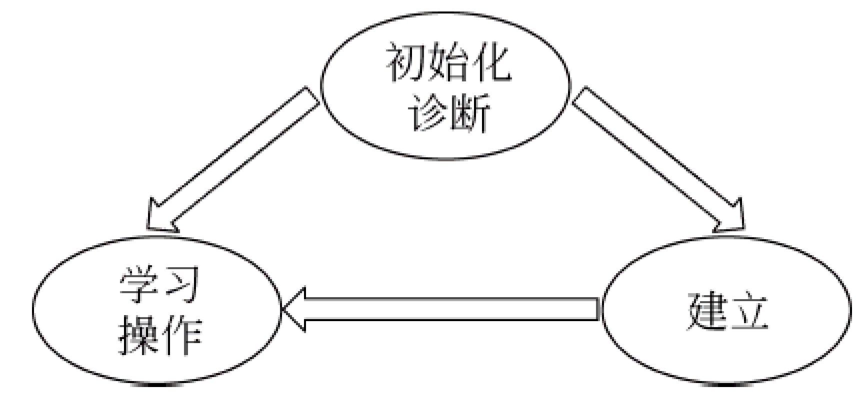


图 6.13　IDEAL 模型示意图

(2) Diagnosing(诊断)。该阶段主要工作为理解

组织当前和期望的过程成熟度状态，这些是形成组织过程改进行动计划的基础。

(3) Establishing(建立)。该阶段主要工作为基于努力目标和诊断阶段开发的建议来制定详细的行动计划，计划必须考虑各种约束。

(4) Acting(操作)。即实施阶段。无论是资源还是时间，都需要各方面付出最大程度的努力。

(5) Learning(学习)。该阶段既是本次循环的终止，又是下一次改进过程的开端。对整个过程改进活动进行评估。

6.2.4 SSAM 体系与原理

1. SSAM 的概念

SSE-CMM 评估方法(SSE-CMM Appraisal Method，SSAM)，是作为专门基于 SSE-CMM 的评估方法。它包含评估一个信息安全工程组织的工程过程能力和成熟度所必需的信息及指南，可用于组织级评估，也可用于项目级的评估。

SSAM 使用多重数据采集方法获得被评估组织或项目中所实施过程的相关信息，如采集途径可以包括问卷调查、人员访谈、证据分析等。

2. SSAM 的参与者

SSAM 的参与者包括发起组织、评估组织和被评估组织。

(1) 发起组织。发起组织的主要工作包括：定义评估范围和目标；从评估组织中选择可用的评估方案和对 SSE-CMM 模型进行裁减以适应需要。

(2) 评估组织。评估组织的主要工作包括：提供从事评估工作的人员；协助发起方选择合适的评估方案以及裁减 SSE-CMM；注意保持客观态度，不要把偏见带入工作中。

(3) 被评估组织。被评估组织也就是接受评估的组织，被评估组织的主要工作通常由发起方给出评估要求的时候确定，或者由竞标会上投标的评估组织给出。

3. SSAM 的评估类型

目前，SSAM 的评估类型主要由三方评估和自评估组成。三方评估是指发起、评估与被评估组织是不同的 3 个组织；而自评估是指发起、评估与被评估组织都是同一个组织。

使用哪种评估应该按照评估的目的确定：如果是为了自身工程能力的改进，适宜使用自评估；如果评估目标是下列中的一种，要考虑进行三方评估。

(1) 基于工程合同的要求，考察合作方的资格。

(2) 独立的比较供应商，看谁最具有资格。

(3) 基于检验目的，评估已有供应商。

(4) 确保用户的期望被理解和满足。

(5) 在理解供应商弱点的基础上，管理项目风险。

4. SSAM 的评估阶段

SSAM 的评估阶段，主要包括计划阶段、准备阶段、现场阶段和报告阶段四部分，具体内容如图 6.14 所示。

(1) 计划阶段。本阶段主要包括确立评估范围、收集初步证据和制定评估计划 3 个部分。

① 确立评估范围。确定评估对象和评估界限，以满足发起者制定的评估目标。

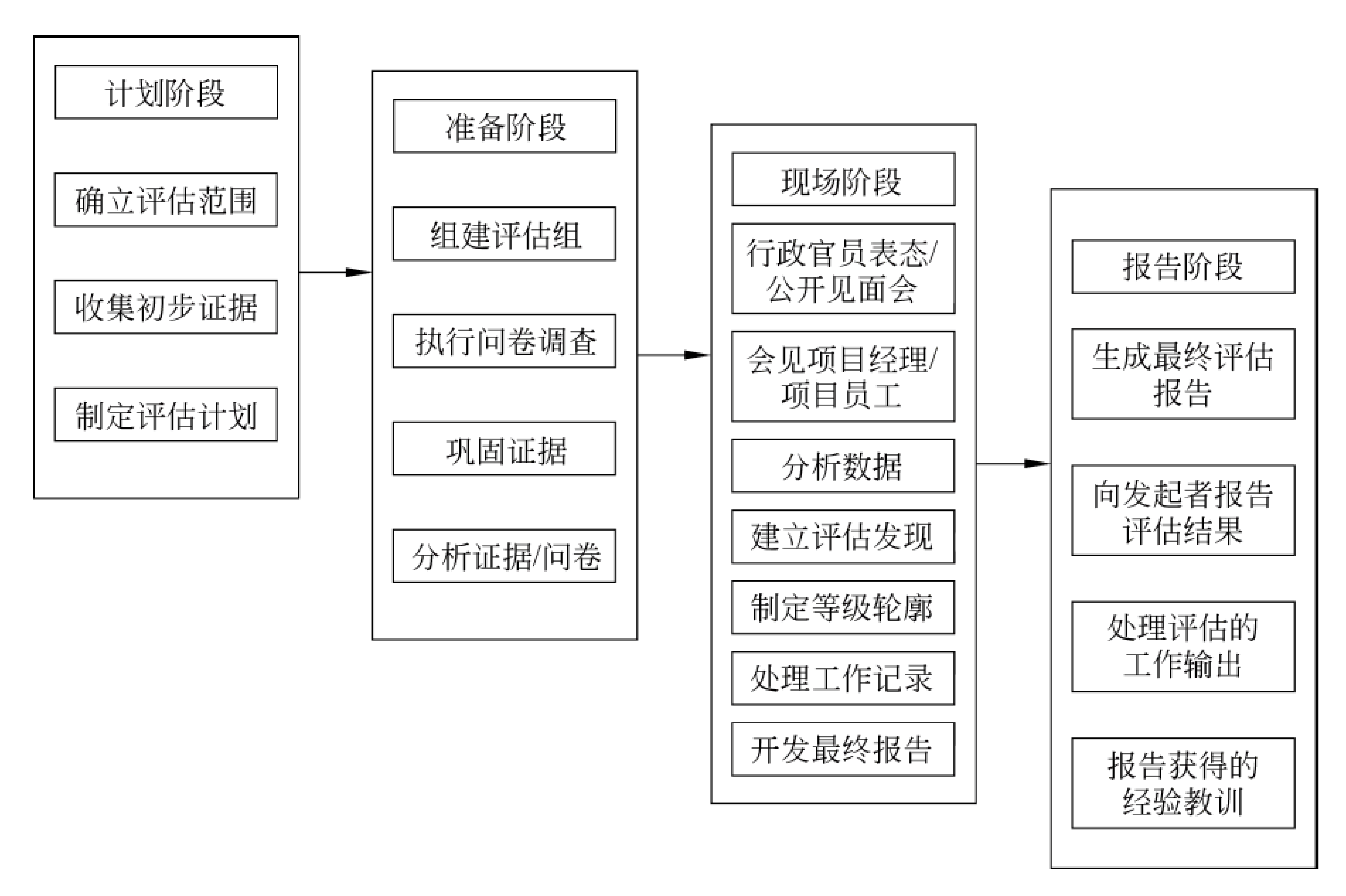


图 6.14　SSAM 的评估阶段

② 收集初步证据。确保在已定义的评估范围内需要的证据都被收集到。

③ 制定评估计划。提出和审议通过最终的评估计划，并把参数和细节记入文档。

(2) 准备阶段。本阶段主要包括组建评估组、执行问卷调查、巩固证据和分析证据/问卷 4 个部分。

① 组建评估组。让评估组里的每一个人都熟悉评估的内容。

② 执行问卷调查。开始进行问卷调查工作，获取被评估组织的一些信息。

③ 巩固证据。把问卷调查获得的数据转录为可分析的格式，以便鉴别和收集支持证据(即支持问卷回答的证据)。

④ 分析证据/问卷。分析由被评估组织提供的问卷回答和支持证据，以便制定在与项目经理会谈时要提出的探索性问题。

(3) 现场阶段。本阶段主要包括行政官员表态/公开见面会、会见项目经理/项目员工、分析数据、建立评估发现、制定等级轮廓、处理工作记录、开发最终报告 7 个部分。

① 行政官员表态/公开见面会。向高级别的行政官员介绍评估过程和日程安排，之后把评估过程和进度展示给所有参与评估的人，同时让行政官员介绍他们对评估的支持。

② 会见项目经理/项目员工。请项目经理就先前所做出的问卷回答做详细阐述。这是通过评估组提出先前确定的探索性问题来实现的，项目经理就探索性问题一一给出回答，并澄清评估组的疑问。消化吸收在与项目经理的会谈中得来的信息，并且将其转化为数据跟踪表中的数据，以利于分析。之后会见待评估项目涉及的员工，就先前确认的关键问题进行询问，并识别新的问题。消化吸收与项目成员的会谈中评估组获得的信息，初步为每个过程域确定等级。

③ 分析数据。这一步要求从零开始对数据跟踪表进行彻底复查，讨论相关问题并以公式表述发掘到的信息。

④ 建立评估发现。制定出一系列的评估发现，以反映对评估中累积数据的综合分析成

果。同时解决初步评估发现中的问题，以防止这些问题影响之后等级的判定。

⑤ 制定等级轮廓。在消化吸收初步评估发现和进一步会谈得到的信息的基础上，把数据跟踪表的结果转化为等级轮廓，表述每一个过程域的能力成熟度等级。

⑥ 处理工作记录。将与评估有关的所有记录进行适当处理。

⑦ 开发最终报告。考察过程域和等级轮廓，对本次评估的成果进行总的观察以精炼评估发现，并给被评估组织提供评估结果。

（4）报告阶段。本阶段主要包括生成最终评估报告、向发起者报告评估结果、处理评估的工作输出、报告获得的经验教训 4 个部分。

① 生成最终评估报告。综合被评估组织的资料和评估发现，开发出最终的评估报告来准确反映在评估过程中获得的信息。

② 向发起者报告评估结果。评估组将评估的结果提供给发起者，之后组织者按照发起者的要求给出并讨论评估结论。

③ 处理评估的工作输出。对所有最终的工作输出和现场阶段后仍掌握在评估组手里的资料进行恰当的处理。

④ 报告获得的经验教训。总结本次评估中学到的东西，为以后的评估提供帮助。它给了评估组就评估的全过程与发起者进行交互的机会。

6.3 本章小结

安全工程理论背景部分，主要介绍了系统工程与项目管理基础、质量管理基础和能力成熟度模型基础，系统工程是组织管理系统规划、研究、制造、试验、使用的科学方法，是一种对所有系统都具有普遍意义的科学方法。项目管理则是从项目的投资决策开始到项目结束的全过程进行计划、组织、指挥、协调、控制和评价，以实现项目的目标。质量管理则是指全部管理职能的一个方面。该管理职能负责质量方针的制订与实施。质量管理可以理解为为了实现质量目标，而进行的所有管理性质的活动。能力成熟度模型是对于软件组织在定义、实施、度量、控制和改善其软件过程的实践中各个发展阶段的描述。

安全工程能力成熟度模型部分，详细围绕 SSE-CMM 模型进行介绍。这一模型描述了一个组织的安全工程过程必须包含的基本特性，这些特性是完善安全工程的保证，也是信息安全工程实施的度量标准，同时还是一个易于理解的评估系统安全工程的框架。它将安全工程划分为三类基本的过程域组，即风险、工程和保证。SSE-CMM 体系结构的设计目标是清晰地从管理和制度化特征中分离出安全工程的基本特征。为了保证这种分离，SSE-CMM 模型是两维的，分别称为域维和能力维。而由其发展的 SSAM 则包含评估一个信息安全工程组织的工程过程能力和成熟度所必需的信息及指南，可用于组织级评估，也可用于项目级的评估。

第7章　信息安全工程实践

导入语：本章介绍了安全工程实施实践和信息安全工程监理两部分内容。本章主要知识结构如图7.1所示。安全工程实施实践部分介绍了ISSE安全工程过程、发掘信息保护需求、定义信息保护系统、设计信息保护系统、实施信息保护系统以及评估信息保护系统的有效性。信息安全工程监理部分介绍了信息安全工程监理模型、建立阶段目标和信息安全工程各方职责。

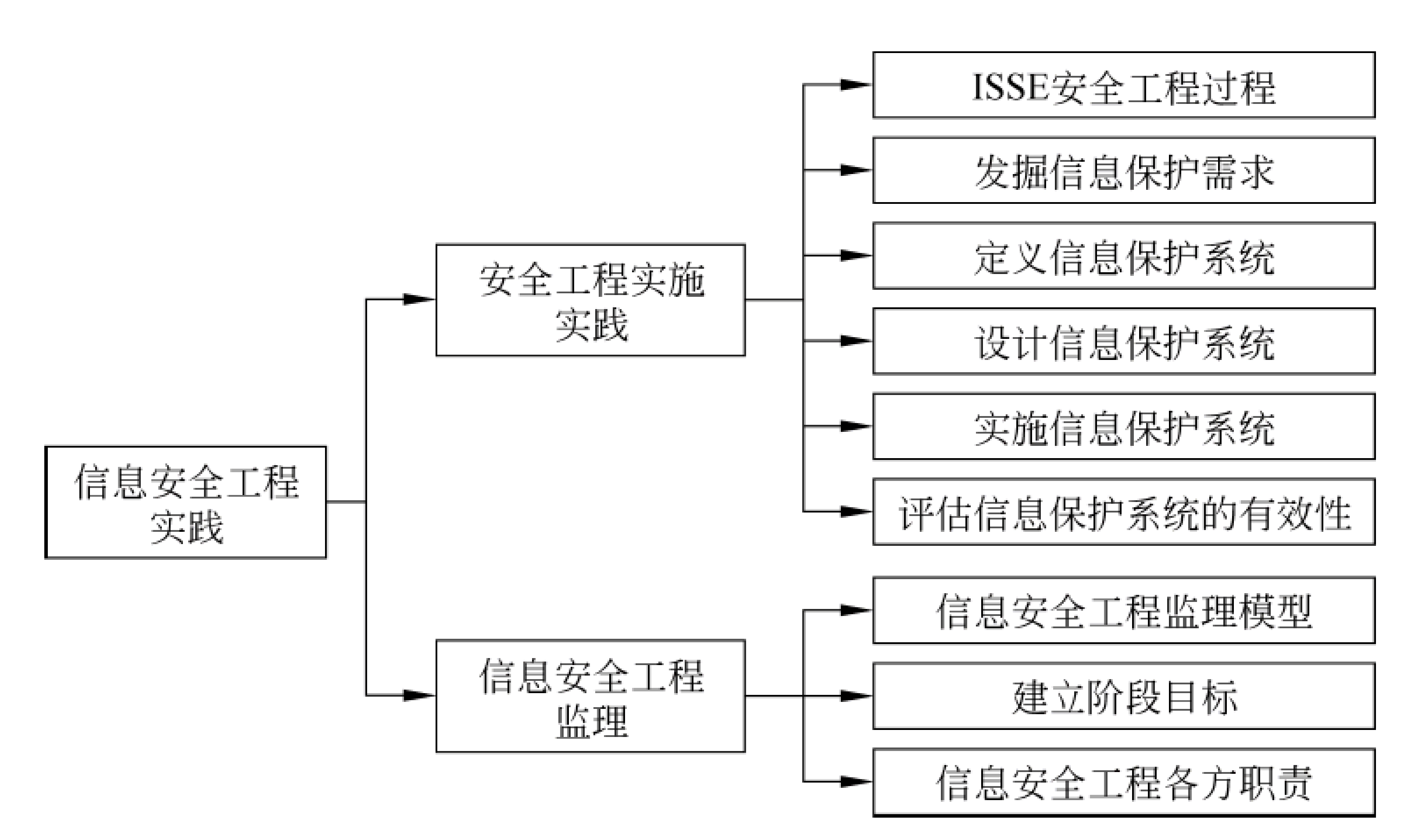


图7.1　本章主要知识结构框图

考核目标：了解系统生命周期的概念和组成阶段：发掘信息保护需求、定义信息保护系统、设计信息保护系统、实施信息保护系统、评估信息保护系统的有效性。理解ISSE的含义：将系统工程思想应用于信息安全领域，在系统生命周期的各阶段充分考虑和实施安全措施。理解ISSE阶段划分及各阶段的主要工作内容；理解风险评估结果是安全需求的重要决定因素；理解国家政策法规和合同协议等符合性要求是安全需求的重要决定因素；理解信息安全必须与信息系统同步规划；理解信息系统用途、架构等特征对安全风险特征的影响；理解信息安全必须与信息系统同步设计；理解根据安全需求有针对性地设计安全措施的必要性；理解信息安全必须与信息系统同步实施、同步运行；理解安全防护措施的部署需要符合总体安全需求和设计方案；理解信息安全工作需要覆盖系统全生命周期；理解持续的风险评估和风险消控是保障系统安全的必要工作。

熟悉信息安全工程监理模型，了解监理阶段目标，了解安全工程各方职责；了解信息安全工程监理工作的意义，了解信息安全工程监理阶段、监理管理和控制手段和监理支撑要素；了解信息安全工程招标、设计、实施和验收阶段监理方的工作目标，了解信息安全工程招标、设计、实施和验收阶段业务单位、承建单位和监理单位的职责和工作流程。

7.1 安全工程实施实践

7.1.1 ISSE 安全工程过程

1. ISSE 安全过程的基本概念

ISSE 是将系统工程思想应用于信息安全领域，在系统生命周期的各阶段充分考虑和实施安全措施。

ISSE 是对信息系统建设中涉及的多种要素按照系统论的科学方法来进行操作的一种安全工程理论，是系统工程学、系统采购、风险管理、认证和鉴定以及生命周期的支持过程的一部分，是系统工程过程的一个自然扩展。

作为一种系统工程技术，ISSE 不仅可以用来设计、实现独立的软硬件系统，还可以为集成的计算机系统的设计和重构提供服务。它可以与设计者和工程人员提供的设计要素以及面向开发者、管理者、用户的接口相结合，在投资额度和成本的限制下，使整体系统获得最大的安全性能。这也反映了对待 ISSE 的实施方法，即总的指导思想是将安全工程与信息系统开发集成起来。

2. ISSE 与 SE 的关系

ISSE 是系统工程(SE)的一个子部分。通常 SE 可以分为概念与需求定义、系统功能设计、系统开发与获取、系统实现与测试和系统维护与废弃 5 个阶段，而 ISSE 过程也分为发掘信息保护需求、定义信息保护系统、设计信息保护系统、实施信息保护系统和评估信息保护系统等阶段。ISSE 与 SE 的关系如图 7.2 所示。

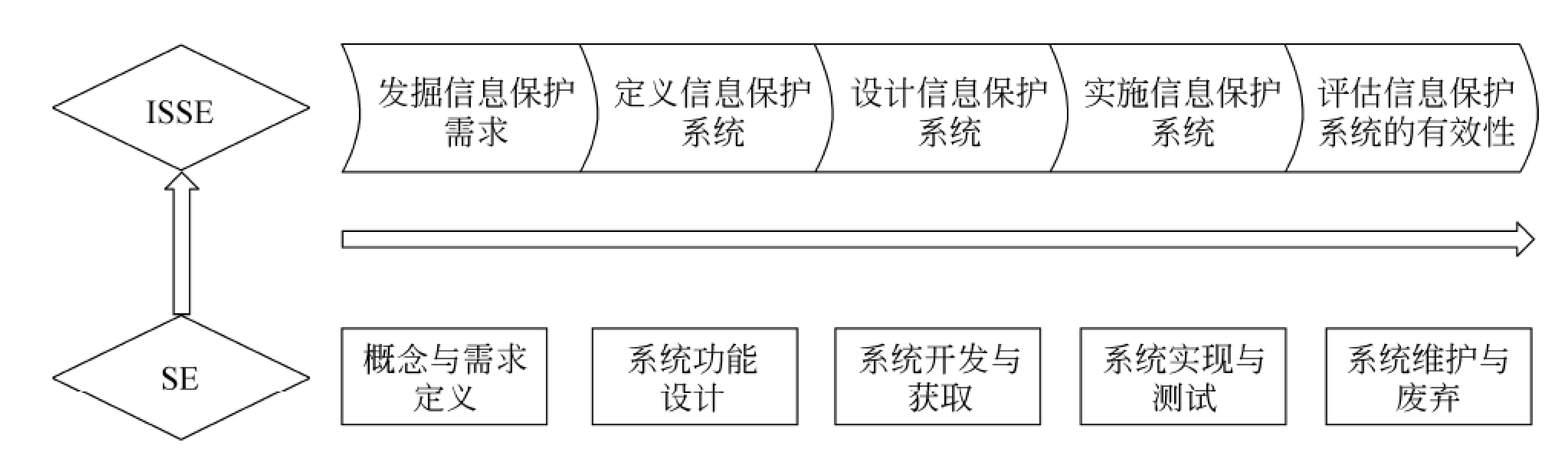


图 7.2　ISSE 和 SE 的关系

3. ISSE 的过程

ISSE 贯穿于系统工程的全过程，这些过程都具有公共的要素：发现需求、定义系统功能、设计系统元素、开发和安装系统、评估系统有效性等。ISSE 的主要活动包括以下内容。

(1) 分析并描述信息保障的用户愿望。

(2) 在系统工程过程的早期，基于愿望产生信息保障的需求。

(3) 确定信息保护的级别，以一个可接受的信息保障的风险水准来满足要求。

(4) 根据需求，构建一个功能上的信息保障体系结构。

(5) 根据物理体系结构和逻辑体系结构分配信息保障的具体功能。

(6) 设计信息系统，实现信息保障的功能构架。

(7) 考虑成本、规划、进度和操作的适宜性及有效性等因素，平衡信息保障风险与其他

的 ISSE 问题。

(8) 研究与其他的信息保障和系统工程原则如何进行权衡。

(9) 将 ISSE 过程与系统工程和采购过程集成。

(10) 测试与评估系统,验证是否达到设计保护的要求和信息保障的需求。

(11) 创建并保留标准化的文档。

(12) 为用户部署系统,并根据其需要调整系统,继续进行生命周期内的安全支持。

为确保信息保障能顺利地被纳入到整个系统,应该从设计系统工程之初便考虑 ISSE,应当随着系统工程的每一个步骤,考虑信息保护的对象、保护需求、功能、构架、设计、实现以及测试等各方面技术和非技术的因素,使信息保障能够在特定系统中得到最好的优化。

ISSE 的体系结构是一个顺序结构,具有严格的顺序性,是按照时间维的发展,即前一项的结果是后一项的输入。违背这种顺序性将导致系统建设的盲目性,最终会导致信息系统安全工程建设的失败。

7.1.2 发掘信息保护需求

发掘信息保护需求首先要了解用户的工作任务需求、相关政策、法规、标准、惯例以及在使用环境中受到的威胁,然后确认系统的用户、他们的行为特点、在信息保护生命周期各阶段的角色、责任和权力等。信息保护的需求应该来自用户的角度,并且不能对系统的设计和实施有过度的限制。一般是通过了解任务的信息保护需求、掌握信息系统可能面临的威胁和考虑信息安全策略等过程来发掘信息安全的需求,如图 7.3 所示。

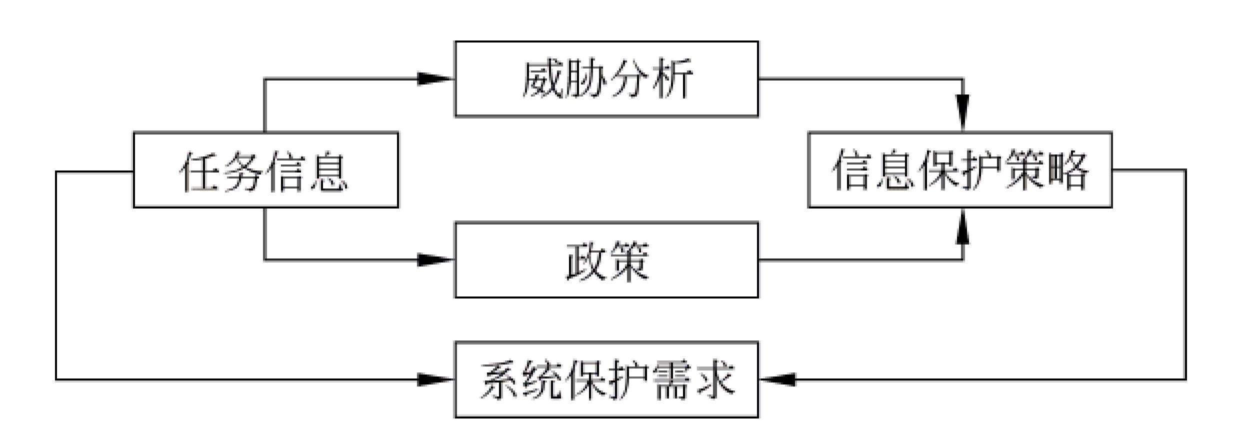


图 7.3 发掘信息保护需求过程框图

1. 了解任务的信息保护需求

ISSE 首先需要考虑系统任务可能受到的各方面的影响(包括人的因素和系统的因素),以及可能造成的各方面的损失,如泄密、数据被篡改、服务不可用、操作抵赖等。

用户通常都明白他们所需要的任务信息的重要性,但在确定这些信息需要何种保护以及达到怎样的保护级别时,可能会一筹莫展。为了科学地了解任务的信息保护需求,需要帮助用户弄清楚什么信息在受到了何种破坏时会对系统的任务造成危害。

在这种要求下,ISSE 需要做到:帮助用户对信息处理的过程建模;帮助用户定义信息所面临的威胁;帮助用户确定信息的保护次序和等级;制定信息保护策略;与用户协调、达成一致。

与用户进行交互是 ISSE 必不可少的环节,在参考用户意见的基础上,评估信息和系统对任务的重要性,并确保任务需求中包含了信息保护的需求、系统功能中包含了信息保护的功能。这个环节要达到的目标是:获得一个满足用户在资金、安全、性能、时间等各方面要求的信息系统保护框架。其中至少要包含以下几个方面:

(1) 被处理的信息是什么？属于何种类型(涉密信息、金融信息、个人隐私信息等)？

(2) 谁有权处理(初始化、查看、修改、删除等)这些信息？

(3) 授权用户如何履行其职责？

(4) 授权用户使用何种工具(硬件、软件、固件、文档等)进行处理？

(5) 用户行为是否需要监督(不可否认)？

在这个环节，ISSE 的工作需要用户的全程参与，共同研究信息系统的角色，使信息系统更好地满足用户的任务要求。

2. 掌握对信息系统的威胁

对信息系统的威胁是指可以利用信息系统的脆弱性，可能造成某个有害结果的事件或对信息系统造成危害的潜在事实。ISSE 需要在用户的帮助下，准确、详尽地定义出在信息系统的设计、生产、使用、维护及销毁的过程中可能受到的威胁。

通过分析信息系统的安全需求，找到安全隐患，应该从以下几个方面入手。

(1) 检测恶意攻击。它指检测人为的、有目的性的破坏行为，这些破坏行为分为主动和被动两种。主动攻击是指以各种方式有选择性地破坏信息，如修改、删除、伪造、乱序等；被动攻击是指在不干扰系统正常工作情况下，进行侦听、截获、窃取、破译等。

(2) 了解安全缺陷。它指了解信息系统本身存在的一些安全缺陷，包括网络硬件、通信链路、人员素质、安全标准等原因引起的安全缺陷。

(3) 掌握软件漏洞。因为软件的复杂性和编程方法的多样性，导致软件中有意或无意留下的一些漏洞，如操作系统的安全漏洞、TCP/IP 协议的漏洞、网络服务的漏洞等。

(4) 分析结构隐患。它主要是指网络拓扑结构的安全隐患，因为如总线型、星形、环形、树形等结构都有各自的优、缺点，都存在相应的安全隐患。

掌握对信息的威胁主体，应该涉及威胁主体的动机或意图、威胁主体的能力、威胁或攻击的途径、主体及威胁存在的可能性及影响或后果。

3. 考虑信息安全的策略

在了解了信息保护需求并掌握了系统面临的威胁之后，ISSE 需要制定出信息安全策略。信息安全策略需要定义出要保护什么、用什么方法保护、如何保护。

制定策略的时候需要全面考虑相关的国家政策、法规、标准和惯例等。为达成这个目标，策略制定小组不仅需要系统工程师、ISSE 工程师、用户代表，还需要信用机构、认证机构、设计专家，甚至是政府机构的参与。

信息安全的策略要提供以下几方面。

(1) 法律和法规。所要遵循的相关法律和法规的要求。

(2) 信息保护的内容和目标。确定要保护的所有信息资源及其重要性、所面临的主要威胁和需要达到的保护等级。

(3) 信息保护的职责落实办法。明确各组织、机构或部门的信息安全保护的责任和义务。

(4) 实施信息保护的方法。确定保护信息系统中的各种信息资源的具体方法。

(5) 事故的处理。包括应急响应、数据恢复等措施以及相应的奖惩条款、监督机制等。

信息安全策略是分层的，一旦制定后，高层的策略一般是不会改变的，而下层的局部策略是可以根据具体情况而定，但不能与更高层的信息安全策略及其他有关政策相违背。

信息安全策略必须由高层管理机构批准并颁布，在策略的贯彻过程中，应该使每个参与者都能够理解策略，并且理解为相同的含义。如果策略在某些地方不能得到贯彻，则一定要让其他参与者都知道这样做的后果。

如某部委每年开展信息安全风险评估工作，定期根据评估结果确定信息安全工程建设项目。评估结果和解决方式如表 7.1 所示。

表 7.1　风险评估案例

风险评估结果	解 决 方 式
市、省、国均可实现网络层未授权的互访	部署防火墙产品
未授权访问过程没有监控和审计措施	部署 IDS 产品
没有能力识别未授权访问所使用的恶意程序代码	部署防病毒产品
私自修改主机、网络设备配置参数	部署网络和主机设备的安全审计产品
内外网混用、私接网线	部署网络准入控制产品
非法复制、篡改数据库数据	部署数据库审计

风险评估结果是安全需求的重要决定因素。一切工程皆有需求，信息安全工程的需求并不是工程的起点，信息安全工程的需求应从风险评估结果分析中得出，需求与风险的一致性越强，则需求越准确。因此信息安全工程应从风险着手，制定需求，这也符合信息安全保障(IA)的思想。

总的来说，发掘信息保护需求的过程如下：分析机构的任务，判断信息对机构任务的关系和重要性；确定法律和法规的要求；确定威胁的类别，判断影响；确定安全服务；记录信息保护需求；记录安全管理的角色和责任；标识设计约束；评估信息保护的有效性；提供文档化的信息保护需求；对信息保护需求的认同；支持系统的认证和认可(C&A)；标识指派的批准官员(DAA)/认可员；标识认证专家(CA)/认证员；确定可适用的 C&A 和采办过程；确保认可员和认证员对信息保护需求的认同。

7.1.3　定义信息保护系统

定义信息保护系统就是要确定信息安全系统将要保护什么、如何实现其功能以及描述信息保护系统的边界和环境的联系情况。任务的信息保护需求和信息系统环境在这里被细化为信息安全保护的对象、需求和功能集合。

一般是通过确定信息保护目标、描述系统联系、检查信息保护需求和功能分析等来定义信息安全系统，如图 7.4 所示。

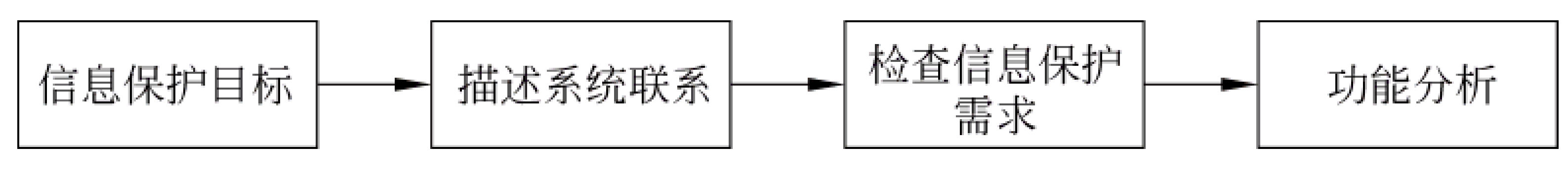


图 7.4　定义信息保护系统的过程

1. 确定信息保护目标

信息保护目标与通常的系统对象具有相同的特性，如对于信息保护需求的明确性、可测量性、可验证性、可追踪性等。确定信息保护对象，要保证它们的这些有效性度量(Measure

of Effectiveness,MoE)性质,在描述每个对象时需要说明以下内容:

(1) 信息保护目标支持系统中的什么任务对象?

(2) 有哪些与信息保护目标和任务相关的威胁?

(3) 失去目标会有什么后果?

(4) 受什么样的信息保护策略或方针的支持?

2. 描述系统联系

系统联系是信息安全系统的边界和环境,即系统与外界交互的功能和接口。在信息安全工程中,系统联系对于确定系统边界并实施保护是很重要的,任务目标、任务信息处理、系统威胁、信息安全策略、设备等都极大地影响着系统边界与环境,因此,描述系统联系需要做以下工作:

(1) 在系统的任务处理过程中,与其他系统和环境之间确定物理的和逻辑的边界。

(2) 描述信息的输入和输出、系统与环境之间或与其他系统之间的信号与能量的双向流动情况。

3. 检查信息保护需求

ISSE 的系统信息保护需求检查任务是对上述过程中的分析(包括目标、任务、威胁、系统联系等)进行特征检查。当信息保护需求从最初的信息保障的用户愿望,经过充分定义,并演变为一系列的系统保护规范时,信息保护的需求能力可能出现缺失,因此,需要检查信息保护需求的正确性、完整性、一致性、依赖性、无冲突和可测试性等特征。

4. 功能分析

ISSE 使用许多系统工程工具来理解信息保护功能,并将功能分配给系统中各种信息保护的配置项。在定义信息安全系统中,对功能进行分析,必须分析备选系统体系结构、信息保护配置项以及信息保护子系统是如何成为整个系统的一部分,这些功能是否能达到原本设定的目标,并理解它们如何才能与整个系统协调工作。

5. 信息安全工程建设

信息安全工程建设应与信息化工程建设同步规划、同步设计、同步实施、同步验收。这是国家的政策要求(国信办【2006】5 号文、发改高技【2008】2071 号文),这是业界的最佳实践,是规避和解决层出不穷的信息安全问题的最有效方式。

信息化建设与信息安全建设脱节的问题,往往是由于对系统缺乏安全方面的认识和了解,没有清晰、完整地定义和描述信息系统,因此信息系统的决策层和管理层应树立以下认识:

(1) “2071 号文”明确提出了电子政务建设项目中的信息安全一票否决制。

(2) “重应用,轻安全”,事前疏于防范,事后追悔莫及。

(3) 安全的发展滞后于业务的发展,是诸多安全问题涌现的“罪魁祸首”。

(4) 方案设计要有安全部分,项目验收要做风险评估。

信息系统用途、架构等特征对安全风险特征的影响:

(1) 任何系统都是有风险的。

(2) 同样一项 IT 技术应用在不同的业务系统中,其风险程度不一定相同,甚至千差万别。

(3) 同等的应用系统,采用不同的技术架构,其安全风险也是不同的。

综上，从信息安全工程保障的角度定义或描述信息系统时，应以保障业务安全的思想为基础，清楚认识业务安全风险以及为业务提供服务支撑的信息系统的安全风险，从而科学、全面地认识信息系统及其安全属性。

7.1.4 设计信息保护系统

明确目标系统后，将构造信息系统的体系结构，详细说明信息保护系统的设计方案，这时 ISSE 工程师要进行功能分配、信息保护预设计和详细信息保护设计等工作，如图 7.5 所示。

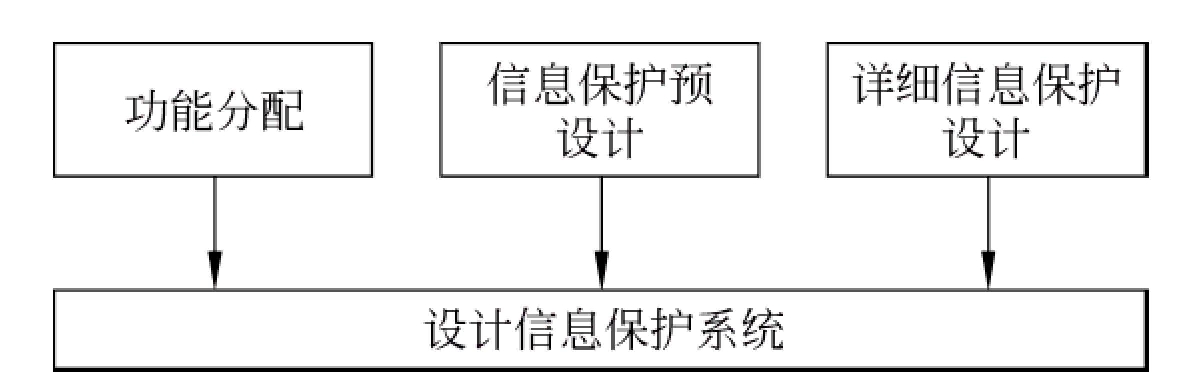


图 7.5 设计信息保护系统的 3 个方面

1. 功能分配

当某种系统功能被定位到人、软件、硬件或固件上后，同时也就附上了相对应的信息保护功能。ISSE 应该为系统制定一个理论和实践上都可行的、协调一致的信息保护系统体系构架。功能分配过程包括以下内容：

(1) 提炼、验证并检查安全要求与威胁评估的技术原理。

(2) 确保一系列的低层要求能够满足系统级的要求。

(3) 完成系统级体系结构、配置项和接口定义。

2. 信息保护预设计

在需求和构架已经确定的前提下，ISSE 进入了信息保护的预设计阶段。在这一阶段，ISSE 工程师将制定出系统建造的规范，其中至少包括：

(1) 检查、细化并改进前期需求和定义的成果，特别是配置项的定义和接口规范。

(2) 从现有解决方案中找到与配置项一致的方案，并验证是否满足高层信息保护要求。

(3) 加入系统工程过程，并支持认证/认可(C/A)和管理决策，提出风险分析结果。

3. 详细信息保护设计

进一步完善配置级方案，细化底层产品规范，检查每个细节规范的完整性、兼容性、可验证性、安全风险和可追踪性等。详细设计包括以下内容：

(1) 精练、验证并检查安全要求与威胁评估的技术原理。

(2) 确保一系列的低层要求能够满足系统级的要求。

(3) 支持系统级体系结构、配置项和接口定义。

(4) 支持长研制周期和前期的采购决策。

(5) 定义信息保护的检验和认证的步骤及战略。

(6) 考虑信息保护的操作和生命周期支持问题。

(7) 继续跟踪、精炼信息保护相关的采办和工程管理计划及战略。

(8) 继续进行面向具体系统的信息保护风险审查和评估。

(9) 支持认证和认可过程。

（10）加入系统工程过程。

信息安全建设是信息系统建设过程的重要组成部分，忽视了安全的信息化建设是不完整的；信息系统建设与信息安全建设同步设计可以避免重复投资、增强效益。

根据安全需求有针对性地设计安全措施是非常必要的。这是因为：

（1）安全设计要依据安全需求。

（2）安全设计要具备可行性和一定的前瞻性。

（3）达到风险—需求—设计的一致性和协调性。

7.1.5 实施信息保护系统

这一阶段的目标是，将满足信息安全需求的信息保护子系统中的各配置项购买或建造出来，然后组装、集成、检验、认证和评估其结果，如图7.6所示。

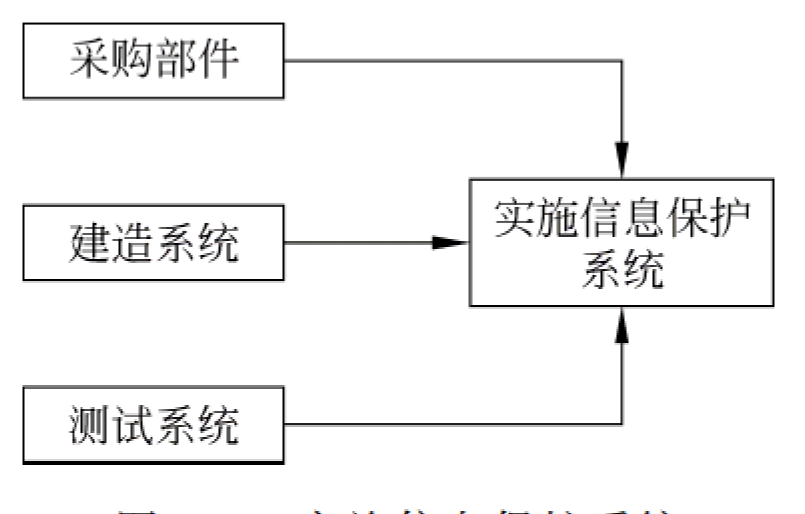


图7.6 实施信息保护系统

1. 采购部件

一般来说，要根据市场产品的研究、偏好和最终的效果，来决定是购买还是自行生产的方式来取得部件。购买/生产的决定应该通盘考虑安全因素、可操作性、性能、成本、进度、风险等影响。在购买时，对于大量生产且相对低成本的商业现货供应COTS(Commercial-Off-The-Shelf)和由政府机构创建的技术团体开发的政府现货供应GOTS(Government Off-The-Shelf)等都可作为部件采购的考虑范围。在采购部件时，要注意考虑以下因素：

（1）确保考虑了全部相关的安全因素。

（2）查看现有产品是否能满足系统部件的需求，最好有多种产品可供选择。

（3）验证一系列潜在的可行性选项。

（4）考虑将来技术的发展，新技术和新产品如何运用到系统中去。

2. 建造系统

建造系统的过程，是确保已设计出必要的保护机制，并使该机制在系统实施中得以实现。与许多系统一样，信息保护系统也会受到许多因素的影响来加强或削弱其效果，这些因素决定了信息保护对系统的适宜程度。所以在建造系统中，要重视以下问题。

（1）部件的集成是否满足系统安全规范？

（2）部件的配置是否保证了必要的安全特性，以及安全参数能否正确配置以便提供所要求的安全服务？

（3）对设备、部件是否有物理安全保护措施？

（4）组装、建造系统的人员是否对工作流程有足够的知识和权限？

3. 测试系统

ISSE要给出一些与信息保护相关的测试计划和工作流程，还要给出相关的测试实例、工具、软硬件等，这些测试系统的工作包括以下内容。

（1）检查、细化并改进设计信息安全系统的阶段结果。

（2）检验解决方案的信息保护需求和约束限制等条件，并实施相关的系统验证和确认机制与决策。

(3) 跟踪实施与系统实施和测试相关的系统保障机制。

(4) 鉴别测试数据的可用性。

(5) 提供安全支持计划,包括逻辑上的、有关维护和培训等方面。

(6) 加入系统工程过程,并支持认证/认可(C/A)和管理决策,提出风险分析结果。

安全工程应重点把握风险、需求、设计、实施的一致性和协调性。

7.1.6 评估信息保护系统的有效性

1. 风险评估

风险评估是重要系统验收和投入运行前的必要工作。

(1) 系统验收引入风险评估机制是政策的要求。

(2) 风险评估是确保和验证安全措施实现的重要手段。

设计和部署的信息安全措施应发挥应有的作用。

(1) 信息安全工程就是产品部署,部署上架后就可以签字验收,使用和配置是运维的事情(错误认识)。

(2) "安全措施"必须予以落实才可以称为安全措施。

(3) 安全措施与应用系统同时落实才能发挥其安全作用。

安全与效率的关系是互相促进的,系统的效率是靠安全来保障的,以牺牲安全为代价换取系统效率的短视行为:

(1) 部署了防火墙产品,但为了视频会议不受"影响",策略为透明全通模式,短时的畅通换来的是病毒泛滥、入侵频发及网络瘫痪。

(2) 只有安全与应用同步运行,才能使安全发挥最大效益,同时也使应用得到最好的保护。

信息安全工程常伴有"影响效率或隐私"的阻力,应正确认识、做好宣讲、果断行事、长痛不如短痛以确保长治久安。

系统验收引入风险评估机制是政策的要求,为落实《国家电子政务工程建设项目管理暂行办法》对风险评估的要求,文件《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》提出了具体要求(相当于"信息安全审计"):

(1) 电子政务工程建设项目应开展信息安全风险评估工作。

(2) 项目建设单位应在试运行期间开展风险评估工作,作为项目验收的重要依据。

(3) 项目验收申请时,应提交信息安全风险评估报告。

信息安全工作需要覆盖系统全生命周期。信息安全工作不是一劳永逸的,需要在全生命周期予以重视;要与风险管理、安全保障等思想相结合,综合认识信息安全问题。

持续的风险评估和风险控制是保障系统安全的必要工作。持续的风险评估是信息安全保障的一项基础性工作;持续的风险评估为新的安全决策和需求提供重要依据。

2. 有效性评估的内容

ISSE 强调了信息保护系统的有效性,主要是指系统在保密性、完整性、可用性、不可否认性等安全特性方面的有效性。如果系统在这些方面达不到要求,信息系统安全工程的任务则很难达到用户的满意。有效性评估要着重以下几点。

(1) 系统的互操作安全性,即系统是否通过外部接口正确地保护了信息。

(2) 系统的可用性，即系统是否能给用户提供信息资源与信息保护。

(3) 用户需要接受什么样的培训才能正确地操作和维护信息保护系统。

(4) 人机界面或接口是否有缺陷，从而导致出错。

(5) 建造和维护信息系统的成本是否可以接受。

(6) 确定风险和可能的任务影响，并提供报告。

7.2 信息安全工程监理

7.2.1 信息安全工程监理模型

社会经济的快速发展，导致各种信息安全问题频繁出现。另外，随着我国对信息安全事务的认同和重视，对信息安全的法律意识与法治建设方面在日益加强与完善，政府在信息安全管理上的发展速度也不断加快。因此，无论建设的信息系统规模大小，在建设之初、建设中以及建设完成后的运维阶段信息系统的安全问题，都已经成为用户关注的重点。作为监理机构在系统建设时，了解并掌握与信息系统安全有关的规定、政策，并在监理过程中加以应用，是保证项目完成预定目标的关键。

1. 信息安全工程监理工作的意义

认真实施信息安全工程监理制度的意义是重大的。它无论是对国家、对建设单位（业主）还是对施工单位（承包商），都是有明显的积极意义的。

(1) 对国家来说，建立具有中国特色的信息安全工程建设监理制度，必将提高投资效益和建设水平，确保国家信息安全建设计划和工程合同的实施，建立起信息化和信息安全领域的新秩序。

(2) 对于建设单位（业主）来说，可以使其筹建机构大大精简，既节省人力、开支，又可使工程得到有效、优质的管理。

(3) 对于监理机构，可以充分发挥其技术、管理等方面智力密集的优势，服务好建设单位，从而创造出最好的社会效益。

(4) 对施工单位（集成商）来说，在其与得到建设单位委托的监理机构打交道，在技术上、管理上可以有共同语言，即使发生争议，也比较容易按现行专业法规去妥善处理，将减少或杜绝过去甲、乙双方之间那种不正常的“扯皮”，而提高施工及管理的效率。

2. 信息安全工程监理阶段、监理管理和控制手段及监理支撑要素

在信息安全工程监理工作方法中，“控制”是最为重要的一个环节，结合以往的经验，监理所实施的控制主要包括两方面：一是参考国际、国内或行业标准及法规政策，建立相关的评判准则；二是按照确定后的评判准则，采用阶段性评审、评估以及适时检查等手段，监督实施过程质量的保证与管理的执行。有效建立具体的准则并开展相关的检查与监督工作，关键在于是否对信息系统安全有关的系统、产品、人员等方面有清晰的认识。信息安全工程监理阶段、监理管理和控制手段以及监理支撑要素如图 7.7 所示。

3. 监理范围

(1) 信息安全工程监理内容范围是信息安全工程，并不专注于某一产品的性能和功能。需要查验以下内容。

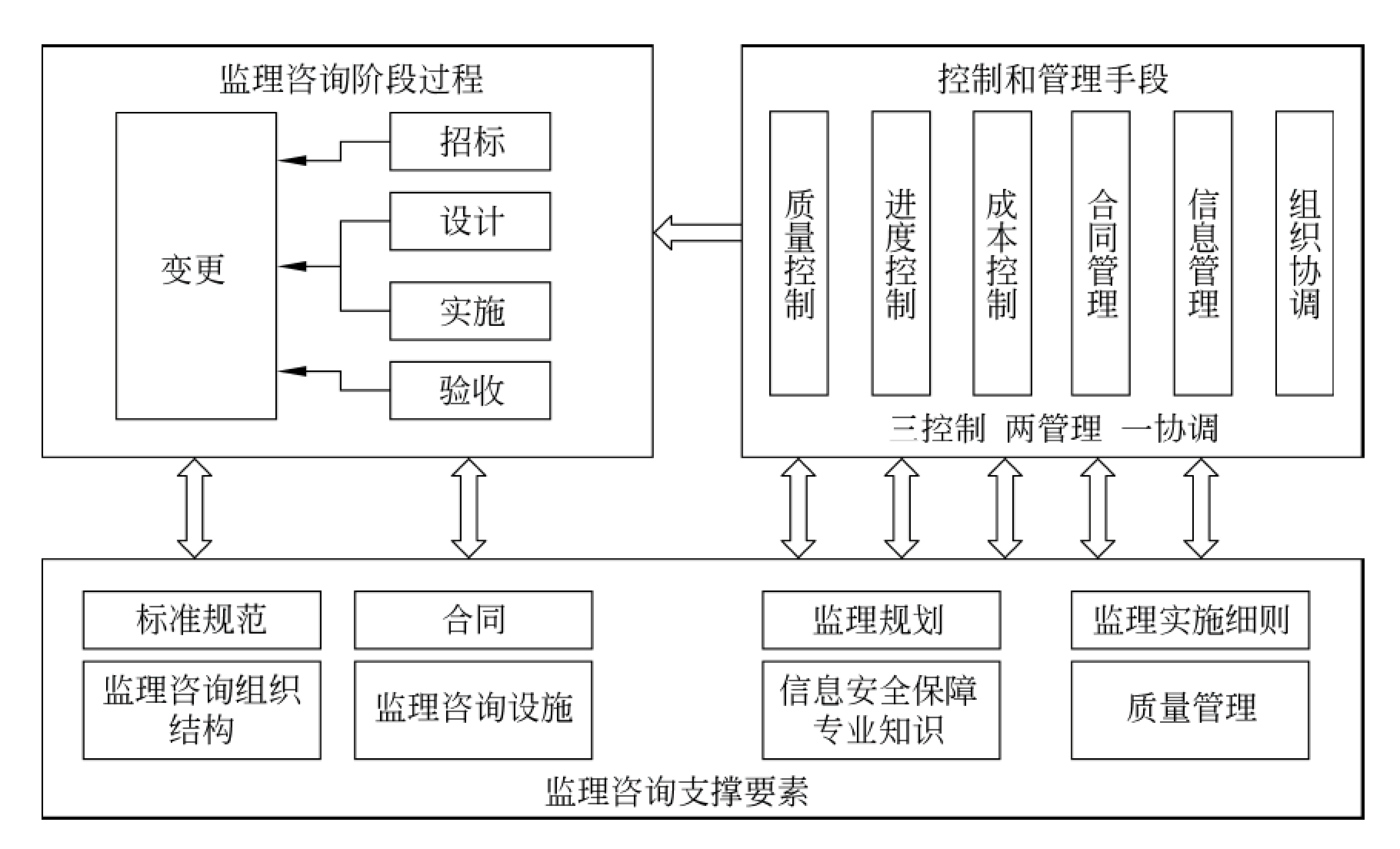


图 7.7　关系图

① 查验产品型号与合同型号是否一致。

② 查验货品及配件是否完好无破损。

③ 查验产品是否能够通过加电测试。

④ 查验产品部署位置是否与实施方案一致。

⑤ 查验产品配置策略是否与实施方案一致。

（2）信息安全工程监理的时间范围是从签署监理合同开始到工程的结束。业主单位应先选择监理方，再选择集成方，最后选择产品供应方。信息安全工程监理覆盖的阶段为需求、设计、实施和验收，并不包含运维阶段，是全工程实施周期的，不是全生命周期的。

（3）信息安全工程监理的人员对象范围是工程实施各方（业主方、集成方、产品供应方、第三方等）。

7.2.2　建立阶段目标

1. 工程招标阶段的主要监理目标

（1）协助业主单位明确信息安全工程需求，确定工程建设目标。

（2）促使承建单位编制的信息安全方案符合国家和业主单位的相关规定，满足需求，合理可行。

（3）促使业主单位、承建单位所签订合同在技术上、经济上的合理性。

2. 工程设计阶段的主要监理目标

（1）加强工程实施方案的合法性、合理性、与安全工程需求和设计方案的符合性。

（2）促使工程计划、设计方案满足工程需求，符合相关的法律、法规和标准，并与工程建设合同相符，具有可验证性。

（3）协助业主单位、承建单位消除设计文档在进入工程实施前可预见的缺陷。

3. 工程实施阶段的主要监理目标

（1）加强工程实施方案的合法性、合理性、与设计方案的符合性。

（2）促使工程中所使用的产品和服务符合承建合同及国家相关法律、法规和标准。

(3) 明确工程实施计划，对于计划的调整必须合理、受控。

(4) 促使工程实施过程满足承建合同的要求，并与工程设计方案、工程计划相符。

4. 工程验收阶段的主要监理目标

(1) 明确工程项目测试验收方案的符合性(验收目标、责任双方、验收提交清单、验收标准、验收方式、验收环境等)及可行性。

(2) 促使工程的最终功能和性能符合承建合同、法律、法规和标准的要求。

(3) 推动承建单位所提供的工程各阶段形成的技术、管理文档的内容和种类符合相关标准。

7.2.3 信息安全工程各方职责

1. 招标阶段

招标阶段的各方职责如下。

(1) 承建方。提供需求书、需求书报审表、信息安全建设方案、信息安全建设方案报审表。

(2) 监理方。要进行需求审核、方案评审，提供方案评审报告。

(3) 业主方。业主对需求书进行盖章认可，对签认的需求书，监理方协助业主方进行专家评审，提供专家评审意见。

主要完成证据有用户签认的《需求书》，附件为监理方签认的《需求书报审表》以及《信息安全建设方案》、《方案评审报告》和《专家评审意见》，附件为监理方签认的《信息安全建设方案报审表》，其他证据为《风险评估报告》等。咨询服务有同承建方、业主方进行沟通、培训；通过所编制的相关标准、规范和指南文件等协助承建方和业主方更好地编制满足需求、业务要求和相关国家、部门等政策、法规标准和行政要求的相关文件。

2. 设计阶段

设计阶段的各方职责如下。

(1) 承建方。提供信息安全工程实施方案、信息安全工程实施方案报审表、信息安全工程阶段测试方案、信息安全工程阶段测试方案报审表。

(2) 监理方。进行方案审核。

(3) 业主方。对安全工程实施方案签认，签认的实施方案；对安全工程阶段性测试方案签认，签认的方案。

主要完成证据有三方签认的《信息安全工程实施方案》和《安全工程阶段测试方案》，附件为监理方签认的《信息安全工程实施报审表》和监理方签认的《信息安全工程阶段测试方案报审表》。其他证据为《风险评估报告》、《安全工程效益评估方案》等。咨询服务有通过所编制的相关标准、规范和指南文件等协助承建方和业主方更好地编制满足需求、业务要求和相关国家、部门等政策、法规标准和行政要求的相关文件。

3. 实施阶段

实施阶段的各方职责如下。

(1) 承建方。提供安全工程阶段实施细则、实施细则报审表、质量管理计划、质量管理计划报审表。

(2) 监理方。进行安全工程阶段实施细则审核、质量管理计划审核。

（3）业主方。业主确认认可实施细则，业主确认认可质量管理计划。

主要完成证据有监理方签认的《安全工程阶段实施细则》，附件为监理方签认的《实施细则报审表》；以及监理方签认的《质量管理计划》，附件为监理方签认的《质量管理计划报审表》。其他证据是各种工程实施过程文件。监理工作为依据实施方案、实施方案细则和质量管理计划对工程实施过程进行符合性监督和检查。

4. 验收阶段

验收阶段的各方职责如下。

（1）承建方。提供：初验、终验验收方案，验收方案报审表，初验、终验报告，初验、终验报审表。

（2）监理方。进行初验、终验方案审核，以及初验、终验审核。

（3）业主方。业主签认方案，业主签认初验、终验报告。

主要完成证据有三方签认的《初验、终验验收方案》，附件为监理方签认的《初验、终验验收方案报审表》；以及三方签认的《初验、终验报告》，附件为监理方签认的《初验、终验报告报审表》。其他证据为各种工程验收过程文件。

7.3 本章小结

ISSE是对信息系统建设中涉及的多种要素按照系统论的科学方法来进行操作的一种安全工程理论。为确保信息保障能顺利地被纳入到整个系统，应该从设计系统工程之初便考虑ISSE，应该随着系统工程的每一个步骤，考虑信息保护的对象、保护需求、功能、构架、设计、实现及测试等各方面因素，使信息保障能够成功实施。

ISSE过程分为发掘信息保护需求、定义信息保护系统、设计信息保护系统、实施信息保护系统和评估信息保护系统等阶段。ISSE过程存在于完整的系统开发生命周期中，ISSE的实施是以信息系统安全保障工程的实施为载体，指导信息系统安全保障体系的建设，就是在系统生命周期内，对ISSE过程完整计划的具体实现。

在建设该电子政务信息系统时，可以按照ISSE过程的思想，充分考虑对信息系统进行安全需求分析、设计、开发和维护，保障系统在全生命周期内的安全服务。

ISSE的许多思想目前已经被纳入到IATF的体系中，它是一种十分有效的工程方法，对信息安全系统的建设具有独到的指导意义，能够对系统提供全方位的安全保护，使用户对安全具有更大的信心。

信息安全工程的监理是在信息安全工程的开发采购阶段和交付实施阶段为业主单位提供的信息安全保障服务。其主要是在项目准备阶段、项目实施阶段和项目验收阶段通过质量控制、进度控制、合同管理、信息管理和协调，来促使信息安全工程以科学、规范的流程，在一定的成本范围内，按时保质保量地完成，实现项目预期的信息安全目标。

信息安全工程监理模型由三部分组成，即咨询监理支撑要素（组织结构、设施设备、安全保障知识、质量管理）、监理咨询阶段过程和控制管理措施（“三控制、两管理、一协调”，即质量控制、进度控制、成本控制、合同管理、信息管理和组织协调）。

第 8 章　信息安全保障

导入语：本章介绍了信息安全保障和历史、信息安全保障体系、信息安全保障评估框架以及信息安全保障评估建设和实践。信息安全保障和历史部分介绍了信息安全保障的发展历史以及我国在信息安全保障方面所做的工作。信息安全保障体系部分介绍了信息安全保障的构成及其空间特性。信息安全保障评估框架部分介绍了安全模型的发展及特点。信息安全保障评估建设和评估实践部分为本章的重点，主要介绍了信息安全保障建设和评估实践的过程。

本章主要知识结构如图 8.1 所示。

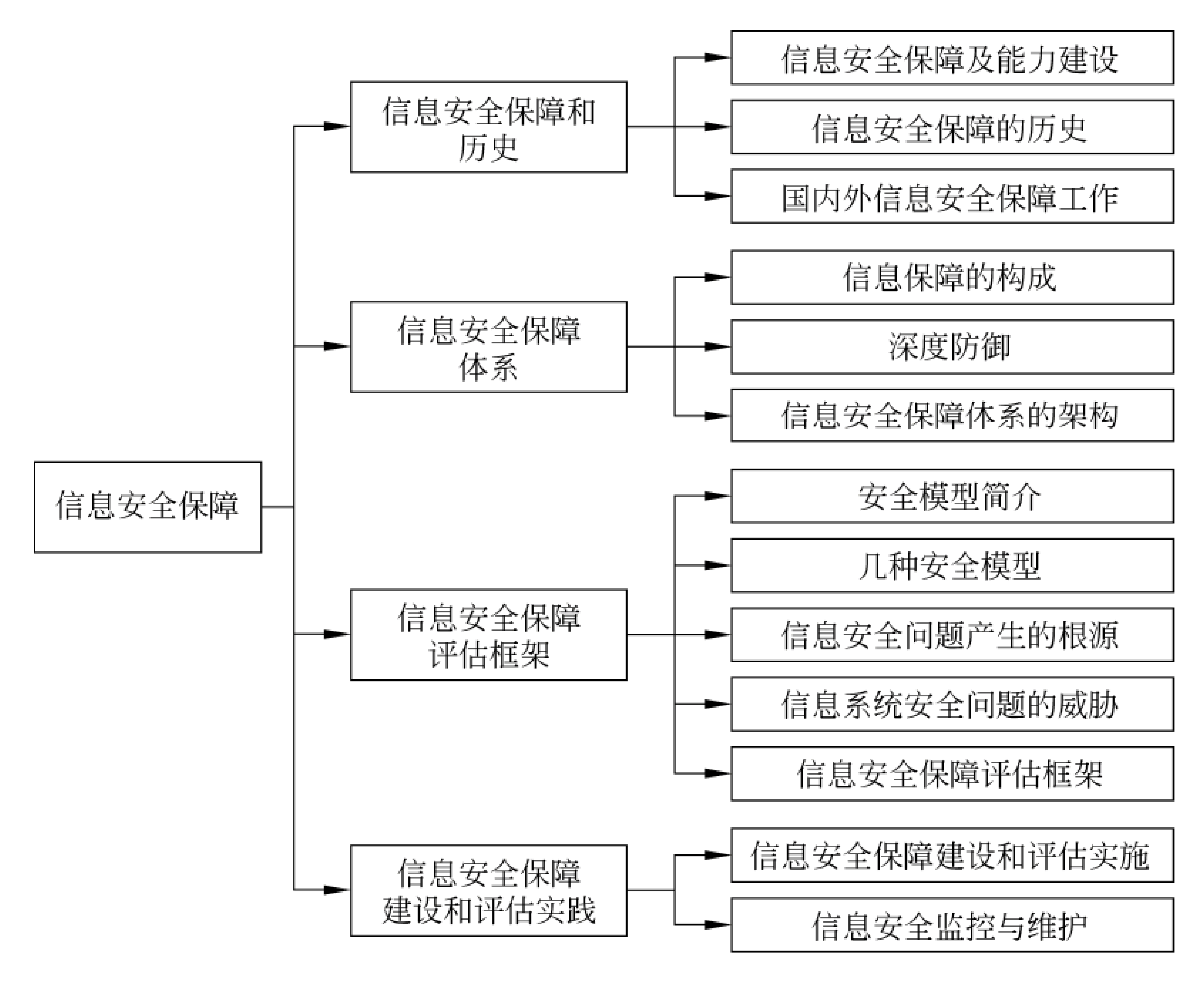


图 8.1　知识结构框图

考核目标：了解信息安全保障的历史；了解信息安全对策必须以风险管理为基础；了解信息安全保障管理体系的建立和分类；了解国内外信息安全保障工作；知道信息保障的构成；理解信息安全保障体系的架构；理解几种安全模型；理解信息系统安全问题产生的根源与环节；掌握信息安全保障评估框架的组成的 4 个部分简介和一般模型、技术保障、管理保障、工程保障；掌握信息系统安全保障建设和评估实施：①确定信息系统安全保障需求，②规范化、结构化描述信息系统安全保障具体需求，③根据信息系统安全保障需求编制具体的安全保障解决方案，④对信息系统安全保障进行评估，⑤用户根据信息系统安全保障评估的结果进行改进；了解国外信息安全保障测评；掌握信息安全监控与维护的主要内容。

8.1　信息安全保障和历史

8.1.1　信息安全保障的历史

信息安全保障，这个词越来越受到人们的关注；据 CNNIC 统计，截至 2011 年 12 月底，中国网民规模达到 5.13 亿，中国手机网民规模达到 3.56 亿，这个庞大的网络群体每天在网上买卖商品，交各种费用、发邮件、聊天、存资料等。其中很多信息是私密的不能让别人知道，但是网络技术日益发达的今天，网络安全成了热门话题。网络上信息不能像是存到银行的保险箱里万无一失的保险，只要黑客技术够厉害，轻而易举地就能拿到任何信息。

信息安全问题始终伴随着信息技术的发展而发展，先后经历了“通信保密”(COMSEC)、“信息系统安全”(INFOSEC)和目前的“信息保障”(IA)3 个阶段。每个阶段虽然在满足的需求、关注的目标及发展技术等方面各不相同。但其根本出发点都是要保护信息的安全。

信息安全保障(IA)的发展历史自 20 世纪 40 年代开始，20 世纪 40～70 年代，信息安全以通信保密为主题，要求实现信息的保密性，该时代标志有 1949 年 Shannon 发表的“保密通信的信息理论”、1976 年 Diffle 和 Hellman 在“New Directions in Cryptography”一文中提出公钥密码体系、1977 年美国国家标准局公布数据加密标准 DES。这一时期的信息安全所面临的主要威胁是搭线窃听和密码学分析，信息安全需求来自军政指挥体系方面的“通信保密”要求，主要目的是使信息即使在被截获的情况下也无法被敌人使用，因此技术主要体现在加密和解密上。

20 世纪 70～90 年代，随着小规模计算机组成的简单网络系统出现，网络中多点传输、处理以及存储的保密性、完整性、可用性问题成为关注的焦点，其时代标志是 1985 年美国国防部发布的可信计算机系统评估保障(TCSEC，橙皮书)，操作系统安全分级(D、C1、C2、B1、B2、B3、A1)；后发展为彩虹(rainbow)系列。这一时期的主要安全威胁扩展到非法访问、恶意代码、脆弱口令等方面，计算机之间的信息交互，要求人们必须在信息存储、处理、传输过程中采取措施，保护信息和信息系统不被非法访问或修改，同时不能拒绝合法用户的服务请求，其技术发展主要体现在访问控制上。这时人们开始将“通信安全”与“计算机安全”合并考虑，“信息安全保障”成为研究热点。

进入 20 世纪 90 年代，随着网络技术的进一步发展，超大型网络迫使人们必须从整体安全的角度去考虑信息安全的问题。网络的开放性、广域性的特征把人们对信息安全的需求延伸到可用性、完整性、真实性、保密性和不可否认性等更安全的范畴。同时，随着网络黑客、病毒等技术的层出不穷、变化多端，人们发现任何信息安全技术和手段都存在弱点，传统的“防火墙＋补丁”这样的方案已经无法安全抵御来自各方的威胁，必须寻找一种可持续的保护机制，对信息和信息系统进行全方位的动态保护。1995 年，美国国防部发现其计算机网络系统遭受了 725 万余次的外来攻击。当时国防部认为，其计算机系统防御能力低下，对袭击的发现概率仅为 12%，能做出反应的还不到 1%，这种紧迫形势引起了美军方的高度重视。1996 年，美国国防部国防科学委员会的一份关于信息战防御能力的评估报告再次指出，国防部网络、信息系统存在很多漏洞和薄弱环节，而且未来还会面临更加严峻的挑战，要

求国防部必须采取特别行动来提高国防部应对现有和不断出现的威胁的能力。为此，1996年美国国防部首次给出了“信息安全保障”的概念，即“保护和防御信息系统中融入保护、检测、响应功能并提供信息系统恢复功能”并把“信息保障”确定为信息优势能力的重要组成部分，在此方针指导下，提出了“信息保障战略计划”，旨在构建一种动态、可持续、全方位的信息保障机制。

进入21世纪，信息时代真正到来，安全变得尤为重要，不仅要求国防高度重视，在日常生活中，也要重视安全的重要性，有可能一不小心就会面临安全威胁。21世纪面临的信息安全威胁主要来自黑客、恐怖分子对利益的渴求，而且这种威胁会延续下去，所以要做好安全保障工作，包括建立技术安全保障体系、建立安全管理体系、培养人员意识等。这一时期标志性技术有美国国防部的IATF深度防御战略等。

8.1.2 信息安全保障及能力建设

信息系统安全保障是在信息系统的整个生命周期中，通过对信息系统的风险分析，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，从而保障系统实现组织机构的使命。

1. 信息系统安全保障能力建设相关概念

如何推进信息系统安全保障能力建设，首先应对信息系统、信息系统安全、信息系统安全保障能力、信息系统安全保障能力建设4个概念有进一步的认识和理解。对概念的深入理解，有利于明确信息系统安全保障能力建设的内容和任务，有利于确定工作范围、方略、思路、方法，有利于制定有关政策和出台有关措施。

(1) 信息系统。这是一个集成的系统，一个组织中信息流动的总和，是根据一定的需要进行信息接收、选择、处理、存储与传递等活动而涉及的所有因素的综合体。它支持与改善组织的日常业务运作，满足管理人员解决问题和制定决策的各种信息需求。这里所提到的信息系统，是基于计算机与通信技术等现代信息技术手段之上的、集组织的各种信息流于一体，并为组织管理提供信息服务的系统。

(2) 信息系统安全。这是信息系统的免疫系统。如果免疫系统不健全，整个系统将是无能的，甚至是有害的。目前，人们对信息系统安全的概念认识进一步加深，即在保证信息系统信息的保密性、完整性和可用性概念的基础上，增加了保证信息和系统的可控性、信息行为的不可否认性。

(3) 信息系统安全保障能力。这是指对整个信息系统和信息进行保护和防御的能力，主要包括对信息系统的预警、保护、检测、应急和恢复5个能力。

(4) 信息系统安全保障能力建设。“建设”在新华字典里的解释是，创立新事业或增加新设施。这里对建设概念的理解，是指实现和提高信息系统安全保障能力，因此它不仅仅是依靠技术单一因素，是人、政策和技术三大因素的结合，它们共同作用于整个信息系统安全保障5个能力环节中，其中人是主体，技术是具体的解决手法，而政策是两者之间的桥梁。

2. 信息系统安全保障能力涵盖的内容

信息系统安全保障能力建设主要包括以下内容。

(1) 预警能力建设。这是指根据所掌握系统的脆弱性和了解当前的犯罪趋势，预测未

来可能受到的攻击和危害。首先要分析威胁来源和方式，信息系统可能存在的脆弱性。其次对信息系统做资产评估，划分信息系统安全等级。“预则利”，分析面临着什么风险，用什么强度的保护可以消除、避免、转嫁这个风险，划分信息系统安全等级。

（2）保护能力建设。这是采用一切技术和管理手段保护信息系统的保密性、完整性、可用性、可控性和不可否认性。根据已划分的信息系统安全等级完善系统的安全功能、安全机制，对系统进行保护。

（3）检测能力建设。这是检查系统存在的脆弱性。如可能提供黑客攻击、病毒泛滥等系统存在的漏洞等。因此，要求具备相应的技术手段，建立检测的策略和制度，形成报告协调机制。

（4）应急能力建设。这是对危及安全的事件、行为、过程及时做出响应处理，杜绝危害进一步扩大，保证信息系统提供正常的服务。

（5）恢复能力建设。这是指通过容错、冗余、替换、修复和一致性保证等恢复技术，对被非法破坏的信息系统和信息进行快速恢复运转。

3. 现状、问题及建议

自2003年以来，我国的信息系统安全保障工作快速发展。2003年9月，中办发[2003]27号文《关于加强信息安全保障工作的意见》，提出建立国家信息安全的十大任务；2004年1月，中央召开全国信息安全保障会议，明确了今后一段时间我国信息安全保障工作的主要内容和工作重点；2004年8月28日，第十届人大第十一次会议通过了《中华人民共和国电子签名法》，并于2005年4月1日起实施，标志我国信息安全建设的法制化进程向前迈出了重要一步；2004年9月，国家四部委联合下发公通字[2004]66号《关于信息安全等级保护的意见》；同年，由国家认监委牵头，联合国家八部委签发国认联[2004]57号文《关于建立国家信息安全产品认证认可体系的通知》，提出对信息安全产品将逐渐实行3C认证（中国强制认证）；2005年4月，国家信息安全产品认证管理委员会在京成立；目前，《信息安全条例》正在起草，《中华人民共和国信息安全法》也正在筹备中。

农业部近几年加大了信息系统安全保障能力建设的力度。2003年按照中办发[2002]17号文的要求，进行了政务内网和政务外网的改造建设，在网络构架上，内网和外网严格实行了物理隔离。先后制定了《农业部计算机信息系统保密管理规定》（农办发[1999]10号）、《农业部信息上公共信息网保密审查规定》（农办发[2000]5号）、《农业部关于加强信息安全保障工作的意见》（农市发[2003]19号）、《中国农业信息网信息发布保密审查实施办法》、《中国农业信息网网上不良信息应急处理预案》、《农业部联网计算机及网络安全管理办法》、《信息中心信息采编处工作制度》、《信息安全保障应急处理总体预案》等文件和规章制度，建立了7×24h信息系统安全保障的值班制度，加强了信息系统安全保障工作。通过技术手段对信息系统安全现状、系统运行状态进行监控，采用传输加密、防火墙、入侵监测、漏洞扫描、防杀病毒、存储备份等技术，基本实现了集中统一的信息系统安全保障管理模式。

但从总体上看，农业部及全国农业信息系统安全保障能力建设方面还是相对薄弱。

（1）网络与信息系统的防护水平不高，应急处理能力不强。

（2）信息安全管理和技术人才缺乏，关键技术整体上还比较落后，安全保障预警和检测方面的工作基本没有开展，保护、应急和恢复等方面的工作还不够深入与完善。

（3）信息安全管理制度和标准不完善。

(4) 资金投入不足,保障信息系统安全的必要设施、设备有所欠缺,如漏洞扫描系统、反垃圾邮件设备还没有配备,网络系统安全评估、信息系统资产评估、信息系统划分安全等级工作均没有开展。

(5) 有些人的信息安全意识不强,信息安全管理薄弱。

(6) 信息安全保障管理机构和组织队伍不健全,制约着信息安全保障工作的进一步开展,也制约着信息安全保障能力的进一步提升。

信息系统是动态的,对应的安全也应该是动态的。如何做到动态的调整并对可能出现的安全问题做出及时快速的反应,尽最大可能把所有潜在的危险消灭于萌芽中,这就需要构建一套完善的信息系统安全保障体系。体系的构建依赖于对信息系统整体安全以及细节安全做全面的量化和把握,并根据业务类型制定相应的安全等级制度,明确安全的重心,从而做到有的放矢。

(1) 加强领导,突出重点,做好规划,建立健全信息系统安全保障管理责任制。目前要重点保障基础信息网络和重要信息系统安全,创建安全健康的网络环境。要提高应急处理能力,按照已有的信息安全保障应急框架,完善、细化各项信息安全保障应急方案。要认真贯彻落实《关于加强信息安全保障工作的意见》(中办发[2003]27 号)和《农业部关于加强信息安全保障工作的意见》(农市发[2003]19 号)文件精神,研究和制定关于农业部信息系统安全保障工作的规划和管理责任制度。

(2) 建立信息安全等级保护制度。从实际出发,综合平衡安全成本和风险,优化信息安全资源的配置,确保重点,建立信息安全等级保护制度。要重视信息安全风险评估工作,对网络与信息系统安全的潜在威胁、薄弱环节、保护措施等进行分析评估,综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素,进行相应等级的安全建设和管理。

(3) 建设和完善信息系统安全监控能力。信息安全监控是及时发现和处置网络攻击、防止有害信息传播、对网络和系统实施保护的重要手段,要建设和完善集中统一的信息系统安全监控能力。

(4) 完善信息系统安全应急处理协调机制。建立健全指挥调度机制和信息系统安全通报制度,加强信息系统安全事件的应急处置工作。重要信息系统建设要充分考虑抗毁性与灾难恢复,制定信息系统安全应急处置预案。灾难备份建设要从实际出发,提倡资源共享、互为备份。要加强信息安全应急支援服务队伍建设,提倡社会力量参与灾难备份设施建设和提供技术服务,提高信息系统安全应急响应能力。

(5) 加强队伍建设。进一步加强对专业技术人员的培训,提高专业技术人员的技术水平和专业技能;进一步充实技术力量、调整人员结构。信息系统安全保障工作,关系到信息安全和保密,信息安全即国家安全,必须建立一支政治可靠、技术精湛、作风优良的技术人员队伍,为确保信息系统安全提供人才保证。

(6) 确保信息系统安全资金投入。信息系统安全建设是信息化的有机组成部分,必须与信息化同步规划、同步建设。各单位在信息化建设中,要同步考虑信息系统安全建设,保证信息系统安全设施的运行维护费用。信息系统建设必须与信息安全建设同步规划和实施建设。上报信息系统建设项目时,要按照有关规定使安全保障方面的投资不低于项目总投资的 15%。

（7）加强制度建设，进一步健全和完善有关信息网络安全保障的规章制度，在信息安全技术相对落后、安全保障设施投入不足的情况下，充分发挥管理和制度等非技术手段的作用，将信息安全渗透到网络的各个环节，以政策法规和规章制度保障信息系统安全。

8.1.3 国内外信息安全保障工作

1. 国内信息安全保障工作

国内纲领性文件“27号文”《国家信息化领导小组关于加强信息安全保障工作的意见》（[2003]27号），简称“27号文”，它的诞生标志着我国信息安全保障工作有了总体纲领，其中提出要在5年内建设中国信息安全保障体系。“27号文”的总体要求坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全。“27号文”的主要任务（重点加强的安全保障工作）：实行信息安全等级保护；加强以密码技术为基础信息保护和网络信任体系建设；建设和完善信息安全监控体系；重视信息安全应急处理工作；加强信息安全技术研究开发，推进信息安全产业发展；加强信息安全法制建设和标准化建设；加快信息安全人才培养，增强全民信息安全意识；保证信息安全资金；加强对信息安全保障工作的领导，建立健全信息安全管理责任制。“27号文”的主要原则立足国情，以我为主，技术与管理并重；正确处理安全与发展的关系，以安全保发展，在发展中求安全；统筹规划，突出重点，强化基础工作；明确国家、企业、个人的责任和义务，充分发挥各方面的积极性，共同构筑国家信息安全保障体系。我国信息安全保障工作具体分为3个阶段。

1）启动阶段

2001—2002年，是我国网络与信息安全事件频发且性质严重的时期，IP电话通信技术被恶意滥用，数据走私和电话骚扰行为猖獗，直接影响政府日常工作和居民正常生活；互联网淫秽有害信息内容充斥。重要信息系统存在诸多安全隐患，卫星通信故障造成美元兑港元汇价异常，引发国内首例网络炒汇纠纷案；深交所因系统崩溃停市半天，造成直接经济损失和社会影响；北京首都国际机场信息系统出现故障，造成上百个航班延误，数万名旅客滞留等。

信息安全事件频发，改变了我国对信息安全状况的认识，即我国面临的信息安全问题已不再是一个局部性和技术性的问题，而是一个跨领域、跨部门的综合性安全问题，更是一个影响国计民生、关乎国家安全与社会稳定的现实问题。为此，2001年，国家信息化领导小组重组，网络与信息安全协调小组成立，我国信息安全保障工作正式启动。

2）展开与推进阶段

2003年7月，国家信息化领导小组根据国家信息化发展的客观需求和网络与信息安全工作的现实需要，制定出台了《关于加强信息安全保障工作的意见》（中办发27号文件），文件明确了“积极防御、综合防范”的国家安全保障工作方针，提出了加强信息安全保障工作的总体要求和主要原则，以及进一步提高信息安全保障工作能力和水平、维护公众利益和国家安全、促进信息化建设健康发展的具体意见。

2003—2005年是我国信息安全保障体系建设深入推进阶段。此阶段，我国信息化建设快速发展，取得了明显成效。基础信息网络已初具规模，金融、税务、海关、能源、交通、国防等领域建成了一批重要信息系统，电子商务和电子政务快速发展，为国民经济和社会发展做

出了积极贡献。尤其是全国信息安全保障工作会议召开之后，各地区、各部门认真贯彻落实会议精神和27号文件要求，各省(区、市)和有关部门陆续建立了网络与信息安全协调小组，研究制定了加强信息安全保障工作的具体措施。国信办、发改委、教育部、科技部、公安部、国家安全部、财政部、信息产业部、广电总局、新闻办、国家认监委、保密局、国密办以及军队有关单位按照协调小组的要求，认真研究制定配套文件和措施，做了大量工作。银行、电力、铁路、海关、税务、证券、民航等重要信息系统的主管部门也都专门制定并落实了措施，加强和改进本系统的信息安全保障工作。信息安全等级保护、信息安全风险评估、网络信任体系建设、信息安全产品认证认可工作、信息安全标准制定、信息安全监控和信息安全应急处理等工作均取得积极推进和明显进展。

3) 深化落实阶段

自2006年至今，国家信息安全保障体系建设取得实质性进展。围绕中办第27号文件开展的各项信息安全保障工作迈出了坚实步伐。信息安全法律法规、标准化和人才培养工作取得了新成果。信息安全基础设施和工程建设进一步完善，信息安全等级保护和风险评估取得了新进展。随着中国信息化进程不断加快，国民经济与社会信息化水平不断提高，信息化在促进经济与社会协调、稳定、持续发展过程中，发挥着越来越重要的作用。我国信息安全保障工作取得了明显成效，建设了一批信息安全基础设施，加强了互联网信息内容安全管理，为维护国家安全与社会稳定、保障和促进信息化建设健康发展发挥了重要作用。目前我国的信息安全保障工作正在稳健、扎实地步入高速发展的新阶段。

我国信息安全保障工作的基本思路是：以维护国家利益为根本出发点，服从和服务于国家发展和安全，适应国内改革开放不断深入的形势和全球信息化加速发展的趋势，坚持以人为本、全面协调可持续的科学发展观，突出保障重点，推动自主创新，实现跨越式发展，走投入较少、效益较高的有中国特色信息安全保障建设和发展之路，为国家发展和社会建设提供有力支撑。坚持用发展、改革和开放的办法解决面临的信息安全问题，从法律、管理、技术和人才等多方面入手，采取多种安全措施动员和组织全社会力量，共同构建国家信息安全保障体系。

我国信息安全保障工作目标包括4个方面。

(1) 保障和促进信息化发展。在实施国家信息化发展战略中，要高度重视信息安全保障体系建设，实现信息化与信息安全协调发展。国家基础信息网络、重要信息系统以及政府、企业和公民的信息活动的安全若不能得到切实保障，信息化带来的巨大经济与社会效益就难以有效发挥，信息化发展也会受到严重制约。加强信息安全保障的目的，就是要保障和促进信息化发展，而不是以牺牲信息化发展来换取信息安全。采取不上网、不共享、不互联互通等传统封闭的方式保安全，会严重影响甚至阻碍信息化发展，也不可能从根本上解决信息安全保障问题。只有继续大力推动信息化建设，全面提高信息化发展水平，才能为应对各种信息安全问题提供强有力的物质和技术保障。全面推进信息化，只有高度重视信息安全保障建设，才能形成健康有序、安全稳定的信息网络秩序，才能确保信息化进程稳步、快速地发展。

(2) 维护企业与公民的合法权益。加强信息安全保障是维护企业与公民合法权益的重视前提和根本保证。《全国人大常委会关于维护互联网安全的决定》、《中华人民共和国电信条例》、《中华人民共和国计算机信息系统安全保护条例》等有关法律、法规，对维护公民的通

信自由、保护企业和公民信息活动的权益都作出明确的规定。依据信息安全问题的发展变化和从保护广大用户安全的需要出发，我国正在进一步修改和完善相关的行政法规和部门规章，《信息安全条例》也即将出台。为切实维护企业和公民信息权益，形成良好、安全、可信的信息网络环境，中国政府执法部门依法严厉打击各种形式的网络违法犯罪活动，包括手机短信诈骗、网络金融欺诈、网上非法传销、滥发垃圾邮件、非法传播“黄”、“赌”、“毒”等。中国政府有关部门也依照相关法律及程序，对信息通信网络的运行实行必要的检测，以有效维护国家信息基础设施和重要信息系统安全。

（3）构建安全可信的网络信息传播秩序。我国是世界上第一大手机和第二大互联网国家。构建更加安全可靠、更加有用、更加可信的互联网，服务于建设小康社会和构建和谐社会，是我国加强信息安全保障的一个重要任务。由于网络信息传播的开放性、跨界性、即时性、交互性等特点，互联网在为广大民众提供和获取越来越多的有用、有益的新闻信息及其他信息服务的同时，也存在着一些虚假和错误导向的新闻信息，以及直接危害公众利益、民族团结、国家统一、社会稳定和国家安全的违法与有害信息及活动。为有效开展互联网治理工作，我国政府提出了互联网管理的基本原则，即积极促进互联网发展，并依法进行管理，鼓励行业自律和公众监督，旨在形成一个可信和安全的互联网信息空间。

（4）保护互联网知识产权。信息通信技术及其应用形式和服务的多样化，移动通信、有线电视及互联网之间的互联互通，有力地加快了信息的交流与共享。信息资源的有效开发和利用，正在不断地满足广大民众在信息、文化、娱乐和生活方面日益增长的需求，极大地发挥了信息化发展带来的经济与社会效益。在促进互联互通和信息共享过程中，保护网络信息内容的知识产权，是中国信息安全保障政策的一项重要内容和目标。

2. 国外信息安全保障工作

当前，随着信息化的不断深入，各国纷纷重视信息安全保障工作，从战略、组织结构、军事、外交、科技等各个方面加强信息安全保障工作力度。在战略方面，发布网络安全战略、政策评估报告、推进计划等文件；在组织方面，通过设立网络安全协调机构、设立协调官，强化集中领导和综合协调；在军事方面，陆续成立网络战司令部，开展大规模攻防演练，招募网络战精英人才，加快军事网络和通信系统的升级改造，网络战成为热门话题；在外交方面，信息安全问题的国际交流与对话增多，美欧盟友之间网络协同攻防倾向愈加明显，信息安全成为国际多边或双边谈判的实质性内容；在科技方面，各国寻求走突破性跨越式发展路线推进技术创新，力求在科技发展上保持和占据优势地位；在保障对象方面，关键基础设施是各国信息安全保障的最核心内容。下面具体介绍各个国家信息安全保障的情况。

1）美国信息安全保障概况

1998 年 5 月，克林顿政府发布了第 63 号总统令（PDD63）：《克林顿政府对关键基础设施保护的政策》。2000 年 1 月，克林顿政府发布了《信息系统保护国家计划 V1.0》，提出了美国政府在 21 世纪之初若干年的网络空间安全发展规划。

2001 年 10 月 16 日，布什政府意识到了“9·11”之后信息安全的严峻性，发布了第 13231 号行政令《信息时代的关键基础设施保护》，宣布成立“总统关键基础设施保护委员会”，简称 PCIPB，代表政府全面负责国家的网络空间安全工作。2003 年 2 月，在征求国民意见的基础上，发布了《保护网络空间的国家战略》的正式版本，对原草案版本做了大篇幅的

改动，重点突出国家政府层面上的战略任务。

2008 年 1 月 2 日，美国发布国家安全总统令 54/国土安全总统令 23，建立了国家网络安全综合计划（CNCI）。

CNCI 计划建立三道防线：

第一道防线，减少漏洞的隐患，预防入侵。

第二道防线，全面应对各类威胁。增强反间能力，加强供应链安全来抵御各种威胁。

第三道防线，强化未来安全环境。增强研究、开发和教育以及投资先进的技术来构建将来的环境。

同时，CNCI 还明确了 12 项任务，包括可信互联网连接（TIC）、网络入侵检测系统、网络入侵防护系统、科技研发、态势感知、网络反间、增强涉密安全、加强网络教育、“超越未来（Leap Ahead）”技术研发、网络威慑战略、全球供应链风险管理机制、公私协作。

美国明确将关键基础设施作为其信息安全保障的重点。关键基础设施定义为关系到美国生死存亡的物理和虚拟的信息系统和资产，这些系统和资产的功能丧失或遭到破坏，会对国家安全、经济稳定、国家公众健康与安全产生严重影响。

目前美国的关键基础设施和主要资源部门包括：信息技术；电信；化学制品；商业设施；大坝；商用核反应堆、材料和废弃物；政府设施；交通系统；应急服务；邮政和货运服务；农业和食品；饮用水和废水处理系统；公共健康和医疗；能源；银行和金融；国家纪念碑和象征性标志；国防工业基地；关键制造业。

美国联邦政府负责信息安全保障工作的最高官员是网络安全协调官，负责领导白宫“网络安全办公室”，制定和发布国家信息安全政策，首任网络安全协调官霍华德·施密特被喻为“网络沙皇”。

美国信息安全管理部门包括国土安全部（DHS）、国家安全局（NSA）、国防部（DOD）、联邦调查局（FBI）、中央情报局（CIA）、国家标准技术研究所（NIST）等 6 个机构，具体执行不同的分管职责。

同时，美国重视公私合作机构的合作，包括国家基础设施顾问委员会（NIAC）、信息共享和分析中心（ISAC）、网络安全全国联盟（NCSA）等。

2）英国信息安全保障概况

2009 年 6 月，英国发布首份国家《网络安全战略》，宣布成立“网络安全办公室”和“网络安全运行中心”，提出建立新的网络管理机构的具体措施。

英国注重信息安全标准组织建设，重视将本国标准向海外推广，积极参与国际信息安全标准制定，其 BSI 7799 标准已成为国际标准，并主导 ISO/IEC 27000 系列标准。

英国在其信息安全保障工作中强调网络监控，规定警方和国家安全、税务等监察部门有权监控电子邮件和移动电话等系统，成为西方大国中唯一的政府可以要求网络用户交出加密资料密钥的国家。

英国的关键基础设施包括：通信；应急服务（救护、消防、警察、营救等）；能源（电力、石油等）；金融；食品；政府和公共服务；公共安全；健康（医疗保健、公共卫生）；交通；水处理。

英国负责基础设施保护的机构是国家基础设施安全协调中心，它是负责信息安全工作的跨部门机构，运行着英国的计算机应急响应小组。信息保障中央主办局和民事应急局是

英国负责信息安全工作的重要政府机构。

在立法工作方面，英国 1984 年制定《数据保护法》，1990 年出台《反计算机滥用法》，1997 年实施《电信诈骗法》，2000 年出台《信息自由法》。

在政策方面，1998 年贸易和工业部发表《加强竞争力白皮书》，确定了英国建设信息社会的方式；2005 年英国政府制定发表了《信息保障管理框架》作为信息安全保障战略。

3）德国信息安全保障概况

德国是世界上第一个建立电子政务标准的国家。1991 年，德国在内政部下建立信息安全局（BSI），负责处理与网络空间相关的所有问题。德国重视关键基础设施信息安全保障，建立日耳曼人的“基线”防御；1997 年建立部际关键基础设施工作组；2005 年出台《信息基础设施保护计划》和《关键基础设施保护的基线保护概念》。

4）法国信息安全保障概况

2003 年 12 月，总理办公室提出《强化信息系统安全国家计划》并得到政府批准实施，其四大目标：确保国家领导通信安全；确保政府信息通信安全；建立计算机反攻击能力；将法国信息系统安全纳入欧盟安全政策范围。

2009 年 7 月 7 日，法国成立国家级“网络和信息安全局”，置于总理领导之下，隶属国防部。

5）俄罗斯保障概况

俄罗斯信息安全重点保护对象包括经济、国内和外交政策、科学和技术、国家信息和通信系统、国防、司法、灾难响应等。

俄罗斯的信息安全管理机构包括：俄罗斯联邦安全理事会；俄罗斯联邦安全局（国家安全管理机关、信息安全工作主管和执法机关）；俄罗斯技术和出口控制局；俄罗斯联邦保卫局、信息技术和通信部。

俄罗斯制定了《俄罗斯国家安全纲要》，将其作为国家信息安全战略，工作中注重安全测评和实施信息安全分级管理。

从上述各国信息安全保障工作情况来看，各国之间历史、国情、文化不同，具体的重点保护对象也有所差异，但共同特点是将与国家安全、社会稳定和民生密切相关的关键基础设施作为信息安全保障的重点；所有国家最常被提到的关键部门都是现代化社会的核心部门，也是被破坏后可能造成极大规模灾害的部门。

少数国家在中央政府一级设立机构专门负责处理网络信息安全问题，如美国；大多数国家信息安全管理职能由不同政府部门的多个机构和单位共同承担；机构单位的设立以及机构在信息安全管理中的影响力，受到民防传统、资源配置、历史经验以及决策者对信息安全威胁总体认识程度的影响。

上述国家在信息安全保障工作中有几个相同点：将信息安全视为国家安全的重要组成部分是主流；积极推动信息安全立法和标准规范建设是主流；重视对基础网络和重要信息系统的监管和安全测评是主流；普遍重视信息安全事件应急响应；普遍认识到公共私营合作伙伴关系的重要性，一方面政府加强管理力度，另一方面充分利用社会资源。

8.2　信息安全保障体系

8.2.1　信息保障的构成

1. 信息保障的概念

“信息保障”(Information Assurance,IA)概念是美国国防部于20世纪90年代率先提出的,后经多次修改、完善,已得到世界范围的广泛认可。就其本质来说,信息保障是一种保证信息和信息系统能够安全运行的防护性行为,是信息安全在当前信息时代的新发展。信息保障的对象是信息以及处理、管理、存储、传输信息的信息系统;目的是采取技术、管理等综合性手段,使信息和信息系统具备机密性、完整性、可用性、可认证性、不可否认性以及在遭受攻击后的可恢复性。

随着人类社会步入信息时代,信息已成为重要的战略资源。信息和信息系统安全已成为21世纪关乎国家安全,特别是军事安全的关键因素。美军认识到,在其军事系统网络化、信息化程度空前提高,并产生巨大军事效益的同时,伴随而来的必定是风险增加、漏洞丛生等“负效应”。曾有报道,美国国防部每年由于计算机网络系统本身以及构建于其上的各种信息系统遭受外来攻击而造成的损失可达几千万甚至几亿美元。更严重的是,美国国防部认为,外界对其计算机系统的攻击行动,已使其大量重要军事信息遭到破坏、窃取和篡改,而且其趋势大有愈演愈烈之势,对其军事安全构成了巨大的威胁。为了应对这些威胁与风险,提高其信息和信息系统防御各类攻击和破坏的能力,20世纪90年代初,美军提出了“信息保障”概念,开始实施“信息保障战略”,并将信息保障确立为其军事转型各个领域的首要任务之一。随着技术的不断发展和认识的不断深入,美军“信息保障”概念的内涵和外延也在实践中不断扩充和延伸,已经从最初的一套简单的纯技术防护措施,发展到现在由“人”、“技术”和“操作”3个范畴共同构成的一个综合体系,包括了政策管理、组织实施、运行使用、基础设施建设等方方面面的内容,成了指导美军构建信息安全体系的重要战略思想。

2. 信息保障是信息安全的新发展

信息安全问题始终伴随着信息技术的发展而发展,先后经历了早期的“通信保密”(COMSEC)、“信息系统安全”(INFOSEC)和目前的“信息保障”3个阶段。每个阶段虽然在满足的需求、关注的目标以及发展的技术等方面各不相同,但其根本出发点都是要保护信息,确保其能为己所用。

20世纪40～50年代,信息安全以通信保密为主体,要求实现信息的机密性。这一时期的信息安全需求基本来自军政指挥体系方面的“通信保密”要求,主要目的是要使信息即使在被截获的情况下也无法被敌人使用,因此其技术主要体现在加、解密设备上。

20世纪60～70年代,随着小规模计算机组成的简单网络系统的出现,网络中多点传输、处理以及存储的保密性、完整性、可用性问题成为关注焦点;计算机之间的信息交互,要求人们必须采取措施在信息存储、处理、传输过程中,保护信息和信息系统不被非法访问或修改,同时不能拒绝合法用户的服务请求,其技术发展主要体现在访问控制上。这时,人们开始将“通信安全”与“计算机安全”合并考虑,“信息系统安全”(INFOSEC)成为研究热点。

进入20世纪90年代,随着网络技术的进一步发展,超大型网络迫使人们必须从整体安

全的角度去考虑信息安全问题。网络的开放性、广域性等特征把人们对信息安全的需求，延展到可用性、完整性、真实性、机密性和不可否认性等更全面的范畴。同时，随着网络黑客、病毒等技术层出不穷、变化多端，人们发现任何信息安全技术和手段都存在弱点，传统的“防火墙＋补丁”这样的纯技术方案已无法完全抵御来自各方的威胁，必须寻找一种可持续的保护机制，对信息和信息系统进行全方位的、动态的保护。1989 年美国卡内基・梅隆大学计算机应急小组开始研究如何从静态信息安全防护向动态防护转变。之后，美国国防部在其信息安全及网络战防御理论探索中吸收了这一思想，并于 1995 年提出了“信息保障”概念。

3. 信息保障的防御机制

总的来说，与以前的信息安全概念相比，信息保障概念的范围更加宽泛。从理念上看，以前信息安全强调的是“规避风险”，即防止发生并提供保护，破坏发生时无法挽回；而信息保障强调的是“风险管理”，即综合运用保护、探测、反应和恢复等多种措施，使得信息在攻击突破某层防御后，仍能确保一定级别的可用性、完整性、真实性、机密性和不可否认性，并能及时对破坏进行修复。再者，以前的信息安全通常是单一或多种技术手段的简单累加，而信息保障则是对加密、访问控制、防火墙、安全路由等技术的综合运用，更注重入侵探测和灾难恢复技术。信息保障是防御范畴的信息作战。

信息作战是信息时代联合作战必不可少的作战样式。美军信息作战的主要目的是保护美军的信息和信息系统，干扰和破坏敌方的信息和信息系统，从而获取并保持信息优势，并有效地将其转换为决策优势，最终为联合部队提供竞争优势。在美军 2006 年版的《联合信息作战条令》中，信息作战包括五大“核心能力”(包括电子战、计算机网络攻击、心理战、军事欺骗和作战保密)、“支援能力”(包括信息保障、物理安全、物理攻击、反情报等)和“相关能力”(包括公共事务、军民关系和外交支持等)。信息作战就是综合运用这些能力，影响、破坏、扰乱和剥夺敌方决策能力，同时保护己方信息和信息系统的一种作战行动。

2006 年版的《联合信息作战条令》是这样解释“信息保障”的综合利用各种保护和防护措施，包括检测、响应、恢复等，确保信息和信息系统的可用性、完整性、真实性、机密性和不可否认性。也就是说，信息保障的最终目的是要确保信息能为己方所用，即使其受到攻击或破坏，也能被及时、有效地恢复。其中，可用性是指信息要能按照授权被访问和使用。破坏信息可用性的基本方法是利用某种方式阻断信息(如破坏网络和有关系统)；完整性是指信息不被篡改、破坏和丢失，保证信息的完整性是信息安全的基本要求，破坏信息的完整性是进行信息攻击的主要目的之一；可控性是指要保证信息系统能以人们可接受的质量水平持续运行，并提供有效的信息服务；机密性是指不能让信息泄露给非授权用户和实体，即使被截获也无法使用；不可否认性是指要能保证对收发信息双方的身份和事实进行确认，任何一方在以后都不能抵赖曾处理过特定数据这一事实。

由此可见，信息作战是信息环境下，以信息和信息系统为作战对象的多种军事行动的集合，它既包括防御保护也包括进攻打击，而信息保障重在防御，即保护信息环境中可为己方使用的信息和信息系统。

8.2.2 深度防御

近 20 年来，以信息技术为核心的高新技术以惊人的速度发展，在军事领域引发了一系列深刻的变革，战争形态从机械化向信息化转变，军队的作战方式和作战手段也呈现出崭新

的面貌。1997 年 5 月，美军首次在官方文件中正式确立了“转型”这一建军思想，提出要“为未来而转型美国部队”，开始了打造一支“灵活的、以网络为中心的、基于知识”的军队的历程。信息保障作为这种转型的一个主要支柱，并主要采用了“深度防御”策略。

1995 年，美国国防部发现其计算机网络系统遭受 725 万余次的外来袭击。当时国防部认为，其计算机系统防御能力相当低下，对袭击的发现概率仅为 12%，能做出反应的还不到 1%，这种紧迫形势引起了美军方高度重视。1996 年 11 月，美国国防科学委员会的一份关于信息战防御能力的评估报告再次指出，国防部网络、信息系统存在很多漏洞和薄弱环节，而且未来还会面临更加严峻的挑战，要求“国防部必须采取特别行动来提高国防部应对现有和不断出现的威胁能力”。为此，1996 年，美军在《联合设想 2010》中，正式把“信息保障”确定为信息优势能力的重要组成。在此指导之下，美国国防部提出“信息保障战略计划”，旨在构建一种动态、可持续、全方位的信息保障机制。之后，美国防部在综合考虑技术可行性、成本效益和组织机制等各方面问题的基础上，提出了“深度防御”(Defense in Depth)策略。

“深度防御”策略包括 3 个范畴，即人、技术和操作。其中，人指管理人员、操作人员和用户，美国国防部要求对他们进行培训教育，培养信息保障意识，并确保对其进行有效的管理；技术是指技术框架以及具体的技术手段和标准，还包括对技术的认证与评估；操作是指对信息和信息系统的监督、评估、探测、警告和恢复等行为。在“深度防御”策略中，网络基础设施、计算环境、飞地边界、支撑性设施是美军确定的 4 个重点防护层面。其中，飞地(Encalve)指采用单一安全机制控制下的物理环境，包括用户设备、服务器、路由器等以及由其构成的局域网，边界是通过局域网相互连接、采用单一安全策略并且不考虑物理位置的局域计算设备。

信息安全保障的“深度防御”的基本思想就是要对攻击者和目标之间的信息环境进行分析，然后在每一层都“搭建”由技术手段和管理策略等综合措施构成的一道道“屏障”，形成连续的、层次化的多重防御机制，保障用户信息及信息系统安全，消除给攻击网络的企图提供的“缺口”。深度防御战略如图 8.2 所示。

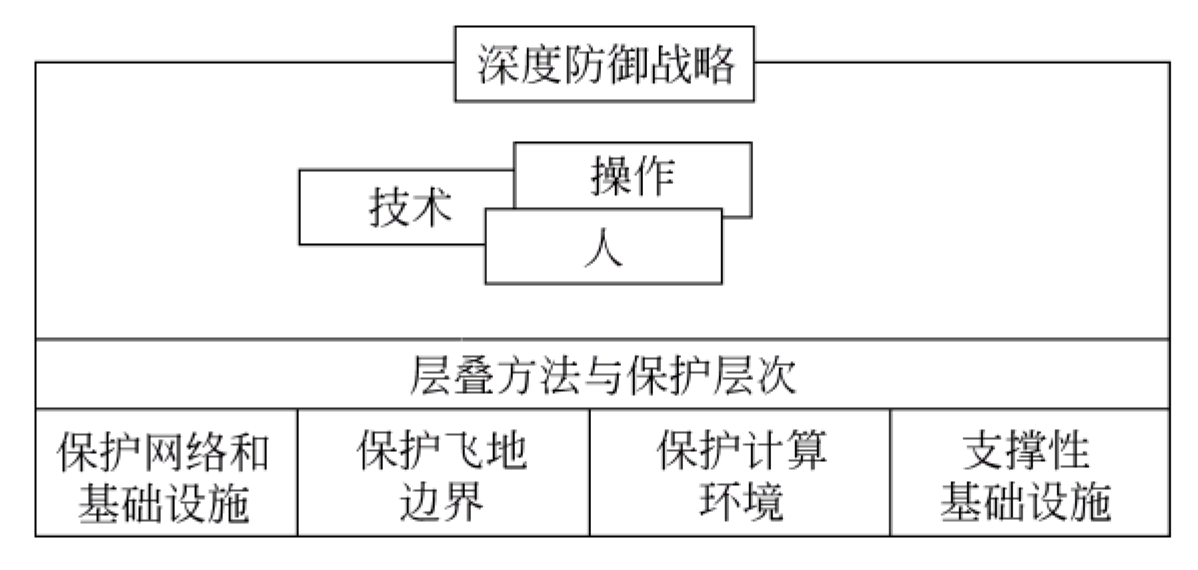


图 8.2　深度防御的信息保障战略

“深度防御”的信息保障战略强调人、技术和操作 3 个核心的原则，对技术和信息基础设施的管理也离不开这 3 个要素。

“深度防御”的信息保障将安全空间划分成 4 个纵深防御焦点域：保护网络和基础设施、保护飞地边界、保护计算环境以及支撑性基础设施，基于“深度防御”的信息保障战略的空间特性来建设信息安全保障体系，需要解决支撑性基础设施、内部网络、网络便捷、网络通信基础设施和主机计算等环境的安全防御问题。

8.2.3 信息安全保障体系的架构

随着信息化的发展，政府或企业对信息资源的依赖程度越来越大，没有各种信息系统的支持，很多政府或企业其核心的业务和职能几乎无法正常运行。这无疑说明信息系统比传统的实物资产更加脆弱，更容易受到损害，更应该加以妥善保护。而目前，随着互联网和网络技术的发展，对于政府或企业的信息系统来讲，是面临着更大的风险和挑战。这就使得更多的用户、厂商和标准化组织都在寻求一种完善的体系，来有效地保障信息系统的全面安全。于是，信息安全保障体系应运而生，其主要目的是通过信息安全管理体系、信息安全技术体系以及信息安全运维体系的综合有效的建设，让政府或企业的信息系统面临的风险能够达到一个可以控制的标准，进一步保障信息系统的运行效率。通常所指的信息安全保障体系包含了信息安全的管理体系、技术体系及运维体系。

信息安全保障体系是实施信息安全保障的法律法规、组织管理、安全技术和安全设施建设等方面有机结合的整体，是信息社会国家安全的基本组成部分，是保障国家信息化顺利进行的基础。信息安全保障体系由管理控制、运行控制和技术控制组合而成，包括 3 种基本要素，即组织要素、内容要素和技术要素。

组织要素包括信息安全保障思想理论基础、信息安全保障主客体、信息安全保障法律基础和信息安全保障体系的管理协调机构。

内容要素包括所有与信息域相关的核心支撑和潜在风险，以及对应的具体安全形态。

技术要素是在信息安全体系中保障信息安全，实现风险描述、管理与控制的所有技术手段及其影响因素的综合。

信息安全保障体系是一个复杂的社会信息系统，基于其组成要素，完整的信息安全保障体系的架构如图 8.3 所示。

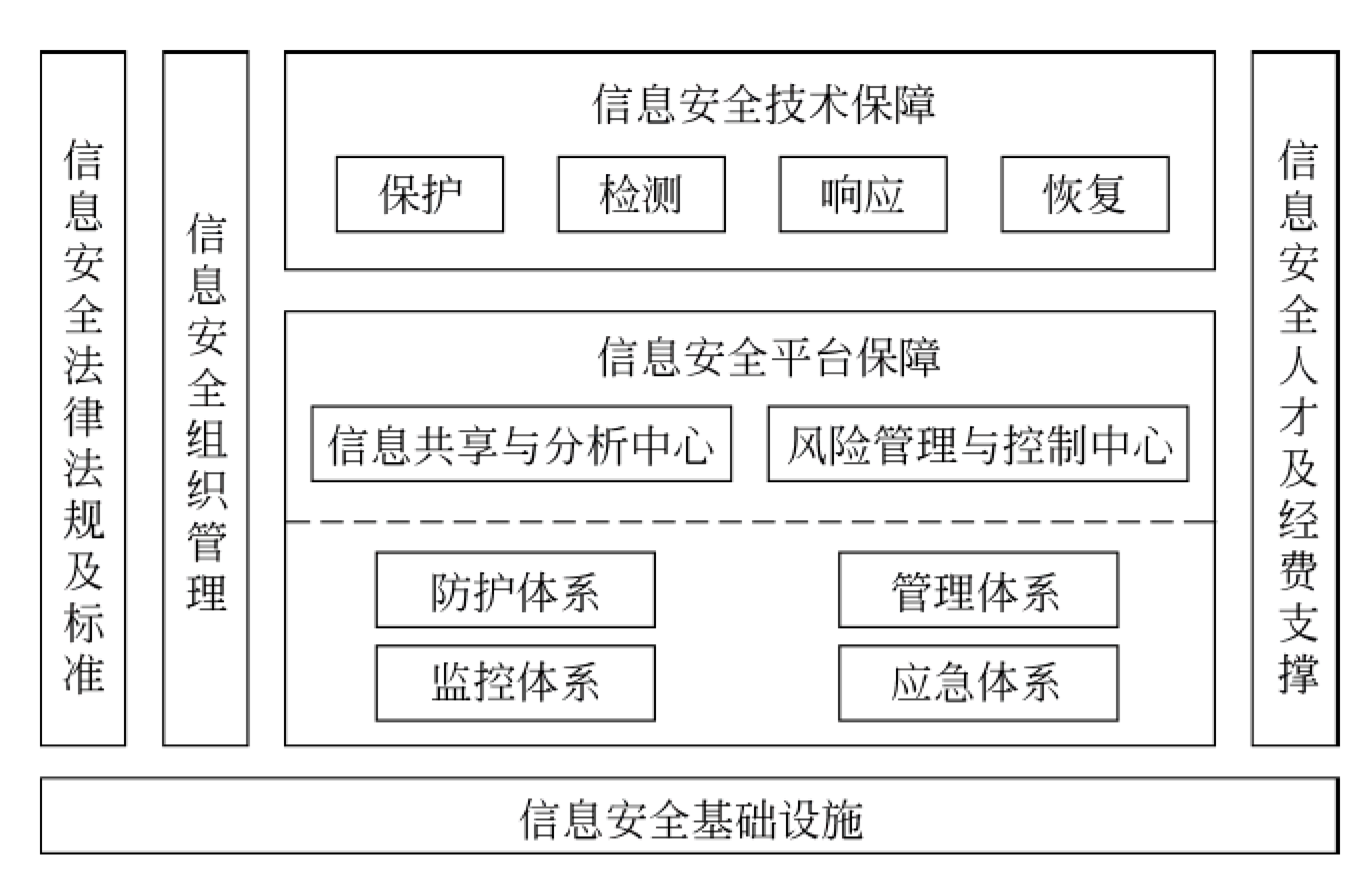


图 8.3 信息安全保障体系架构

如何建立有效的信息安全保障体系呢？需要遵守以下几点。

1）建立 4 个信息安全保障体系

信息安全组织保障体系：建立信息安全决策、管理、执行以及监管的机构，明确各级机构的角色与职责，完善信息安全管理与控制的流程。

信息安全管理保障体系是信息安全组织、运作、技术体系标准化、制度化后形成的一整

套对信息安全的管理规定。

信息安全技术保障体系：综合利用各种成熟的信息安全技术与产品，实现不同层次的身份鉴别、访问控制、数据完整性、数据保密性和抗抵赖等安全功能。

信息安全运维保障体系：在信息安全管理体系规范和指导下，通过安全运行管理，规范运行管理、安全监控、事件处理、变更管理过程，及时、准确、快速地处理安全问题，保障业务平台系统和应用系统的稳定、可靠运行。

2）打造三道防线

第一道防线：由管理体系、组织体系、技术体系构成完备的安全管理体制与基础安全设施，形成对安全苗头进行事前防范的第一道防线，为业务运行安全打下良好的基础。

第二道防线：由技术体系、运维体系构成事中控制的第二道防线。通过周密的生产调度、安全运维管理、安全监测预警，及时排除安全隐患，确保业务系统持续、可靠地运行。

第三道防线：由技术体系构成事后控制的第三道防线。针对各种突发灾难事件，对重要信息系统建立灾备系统，定期进行应急演练，形成快速响应、快速恢复的机制，将灾难造成的损失降到组织可以接受的程度。

3）实现四大保障目标

信息安全：保护政府或企业业务数据和信息的机密性、完整性和可用性。

系统安全：确保政府或企业网络系统、主机操作系统、中间件系统、数据库系统及应用系统的安全。

物理安全：使业务和管理信息系统相关的环境安全、设备安全及存储介质安全的需要得到必要的保证。

运行安全：确保业务和管理信息系统的各种运行操作、日常监控、变更维护符合规范操作的要求，保证系统运行稳定、可靠。

4）遵循 5 个相关国内、国际标准

在信息安全保障体系的建立过程中，充分遵循国内国际的相关标准，即 ISO 27001 标准、等级保护建设、分级保护建设、IT 流程控制管理（COBIT）及 IT 流程与服务管理（ITIL/ISO 20000）。

8.3 信息安全保障评估框架

8.3.1 安全模型

随着信息安全等级保护工作的深入开展，全国范围内重要信息系统定级工作已基本完成，各地区、各部门工作的重点转到了已定级备案信息系统的安全建设整改工作上来。等级保护工作中的安全建设整改是按照国家出台的一系列有关等级保护标准规范，从管理和技术两方面开展信息系统安全建设整改工作，将技术和管理措施有机结合，建立信息系统安全防护体系，提高信息系统整体安全保护能力。

近些年来，国家先后发布了《计算机信息安全保护等级划分准则》（GB 17859—1999）、《信息系统等级保护安全设计技术要求》（GB/T 25070—2010）和《信息系统安全等级保护基本要求》（GB/T 22239—2008，以下简称《基本要求》）等有关信息安全等级保护方面的技术

标准，并要求按照上述技术标准落实各项技术和管理措施。信息系统的安全建设整改是一项涉及信息系统运行使用单位、安全服务商和产品提供商等的复杂系统工程，安全建设整改的参与各方正确理解和使用等级保护的标准规范是有效开展等级保护安全建设整改工作的关键。

随着信息安全技术的发展，信息安全行业流行着各种信息安全体系模型，如 OSI 安全体系结构、PDR 安全保护模型、IATF 信息保障技术框架和 WPDRRC 信息安全模型等，如何正确理解等级保护标准规范中的安全要求（以下以《基本要求》为例说明）和流行安全保护模型之间的关系，如何基于等级保护安全要求针对特定的信息系统量身定做合适的安全防护体系，是制定信息安全解决方案和开展等级保护安全建设整改的基础。

1. 安全模型的概念

安全模型是用于精确和形式地描述信息系统的安全特征，以及用于解释系统安全相关行为的理由。按机制分类可分为访问控制模型、信息流模型等；按服务分类可分为机密性、完整性、可用性模型等。

2. 安全模型的作用

（1）可以准确地描述安全的重要方面与系统行为的关系。

（2）可以提高对成功实现关键安全需求的理解层次。

（3）可以从中开发出一套安全性评估准则和关键的描述变量。

但“安全模型”的表达能力有其局限性，通常的模型是形式语法多于形式语义，甚至只是自然语言的描述。

3. 建立安全模型的方法

（1）信息流模型。其主要着眼于对客体之间的信息传输过程的控制（处于理论阶段）。

（2）访问控制模型。从访问控制的角度描述安全系统，主要针对系统中主体对客体访问及其安全控制。

4. 安全模型的发展

Multics 是 1964 年由贝尔实验室、麻省理工学院及美国通用电气公司所共同参与研发的，是一套安装在大型主机上多人多任务的操作系统。Multics 的目的是想要让大型主机可以达成提供 300 个以上的终端机连线使用，后来因计划进度落后和资金短缺而宣告失败。

BLP 模型是在 1973 年由 D. Bell 和 J. LaPadula 在《Mathematical founda-ons and model》提出并加以完善，它根据军方的安全政策设计，解决的本质问题是对具有密级划分信息的访问控制，是第一个比较完整地形式化方法对系统安全进行严格证明的数学模型，被广泛应用于描述计算机系统的安全问题。

1977 年，K. J. Biba 提出了与 BLP 异曲同工的 Biba 模型，Biba 模型支持的是信息的完整性。

第一个可以实际投入使用安全操作系统是 Adept-50；随后有很多安全操作系统被开发出来。典型的有 Multics、Mitre 安全内核、UCLA Secure UNIX、KSOS 和 PSOS。

8.3.2 几种安全模型

1. 信息流模型

信息流模型实现的关键在于对系统的描述，即对模型进行彻底的信息流分析，找出所有的信息流，并根据信息流安全规则判断其是否为异常流，若是就反复修改系统的描述或模

型,直到所有的信息流都不是异常流为止。信息流模型主要着眼于对客体之间的信息传输过程的控制。需要遵守的安全规则是:在系统状态转换时,信息流只能从访问级别低的状态流向访问级别高的状态。信息流模型的缺点是需要制定输入输出的安全性规范;对具体的实现只能提供较少的帮助和指导。

2. 强制访问控制模型

强制访问控制是"强加"给访问主体的,即系统强制主体服从访问控制政策。强制访问控制(MAC)的主要特征是对所有主体及其所控制的客体(如进程、文件、段、设备)实施强制访问控制。为这些主体及客体指定敏感标记,这些标记是等级分类和非等级类别的组合,它们是实施强制访问控制的依据。系统通过比较主体和客体的敏感标记来决定一个主体是否能够访问某个客体。用户的程序不能改变他自己及任何其他客体的敏感标记,从而系统可以防止特洛伊木马的攻击。强制访问控制一般与自主访问控制结合使用,并且实施一些附加的、更强的访问限制。一个主体只有通过了自主与强制性访问限制检查后,才能访问某个客体。用户可以利用自主访问控制来防范其他用户对自己客体的攻击,由于用户不能直接改变强制访问控制属性,所以强制访问控制提供了一个不可逾越的、更强的安全保护层以防止其他用户偶然或故意地滥用自主访问控制。

强制访问策略将每个用户及文件赋予一个访问级别,如最高秘密级(Top Secret)、秘密级(Secret)、机密级(Confidential)及无级别级(Unclassified)。其级别为 T>S>C>U,系统根据主体和客体的敏感标记来决定访问模式。

3. 多级安全模型

1) BLP 模型

(1) 模型简介。该模型是可信系统的状态—转换模型。定义所有可以使系统获得"安全"的状态集合,检查所有状态的变化均开始于一个"安全状态"并终止于另一个"安全状态",并检查系统的初始状态是否为"安全状态"。该模型是一种机密性访问控制的状态机模型。

(2) 模型定义的主客体访问规则。模型使用状态来表示系统中主体对客体的访问方式;高级别的"可下读,不可下写";低级别的"可上写,不可上读"。

(3) BLP 模型的缺点。只定义了主体对客体的访问,未说明主体对主体的访问,因此该模型无法应用于网络;该模型不能很好地应对隐蔽通道问题。

(4) 应用中的问题。

① 内存管理能够在所有级别进行读和写,在实际应用中有悖于模型本身。除了对它进行"可信假设"外别无他法。

② 当低级别数据写入高级别程序时(即上写),由于模型的限制,低级别主体无法得到任何反馈,仿佛碰到了"黑洞"一般。

③ 文件管理中,重名导致的信息泄露问题。而分立的系统使得 BLP 显得多余。

④ 同样数据库系统中,如果高级别用户发送了一批机密货物到轮船上,而系统不会把这个信息传递给低级别用户(否则就是泄密),那么低级别用户将会认为船是空的,并分配其他货物或改变航行的目的地。

2) Clark-Wilson 模型

(1) 模型简介。

Clark-Wilson 模型偏重于满足商业应用的安全需求,着重研究信息和系统的完整性保

护。其中信息的完整性是指系统中信息的质量、正确性、真实性和精确性,而系统的完整性是指对信息资源成功且正确的操作。主要用于防止授权用户不会在商业应用内对数据进行未经授权的修改、欺骗和错误来保护信息的完整性。在该模型中,用户不能直接访问和操纵客体,而是必须通过一个代理程序来访问客体。从而保护了客体的完整性。使用职责分割来避免授权用户对数据执行未经授权的修改,再次保护数据的完整性。在这个模型中还需要使用审计功能来跟踪系统外部进入系统的信息。

信息的完整性保护有两个方面:组织完善的事务(Well-formed transaction),用户不能随意处理信息,只能在限定的权限和范围内进行;清晰的责任划分(Separation of duty),一项任务需要两个以上的人完成,需要进行任务划分,避免个人欺骗行为。

系统的完整性保护是防止非授权修改,维护内部与外部的一致性,访问授权但不恰当的修改。

(2) 数据分类。被限制数据(CDI),完整性保护的客体;非限制数据(UDI),不需保护的客体。

(3) 访问控制方法。定义可以针对每一个数据(数据类型)完成的访问操作(转换过程);定义可以由主体(角色)完成的访问操作。

(4) 保护方法。

① 完整性确认过程(IVP)。确认数据处于一种有效状态。

② 转换过程(TP)。将数据从一种有效状态改变到另一种有效状态。

③ 如果只有一个转换过程能够改变数据,则该数据是完整的。完整性系统记录所有转换过程,并提供对数据改变的审计跟踪。

实践中,Clark 和 Wilson 提出完整性监控(“证明规则”)和完整性保持(“强制规则”)来实现。前者由管理员来执行,后者由系统来保证。

3) Biba 模型

(1) 模型简介。

Biba 模型是涉及计算机完整性的第一个模型,一个计算机系统由多个子系统组成,而子系统是按照功能或权限将系统(主体和客体)进行划分的,在子系统级进行评估系统的完整性。

系统完整性威胁来源:内部威胁,子系统的一个组件是恶意的/不正确的;外部威胁,一个子系统通过提供错误数据/不正确的函数调用来修改另一个子系统。

Biba 认为可以通过程序测试和检验来消除内部威胁,因此,该模型仅针对外部模型。

(2) 完整性策略;针对客体的最低点策略;最低点完整性审计策略;Ring 策略;严格的完整性策略。

(3) Biba 模型的缺点。Biba 定义的完整性只是一个相对的,而不是绝对的度量。没有使用明确的属性来判断系统是否拥有完整性,它没有关于明确的信息分级的标准。

4. 多边安全模型

1) Chinese Wall 模型

(1) 模型简介。

Chinese Wall 模型访问数据不是受限于数据的属性(密级),而是受限于主体已经获得了对哪些数据的访问权限。将一些可能会产生访问冲突的数据分成不同的数据集,并规定

所有主体最多只能访问一个数据集。而不限制到底选择访问哪个数据集。

(2) 模型安全策略。

主体只能访问那些与已经拥有的信息不冲突的信息。一个主体一旦已经访问过一个客体,则该主体只能访问位于同一公司数据集中的客体,或在不同兴趣冲突组中的信息。在一个兴趣冲突组中,一个主体最多只能访问一个公司数据集。

(3) 模型举例。

有公司 A、B,数据类型分为石油业务数据、银行数据,进行组划分。

访问控制:第一次访问是自由的,不妨设为 A 石油业务数据集;可以访问 A 金融数据集;不可以访问 B 石油数据集。

总结:可以访问与主体曾经访问过的信息同属于同一个公司的数据集,即墙内信息;可以访问一个完全不同的兴趣冲突组。

2) BMA 模型

(1) 模型简介。

BMA 模型由英国医学会(BMA)提出的,由客体同意哪些主体可以有条件地查看并使用客体信息,保证客体信息的完整性和可用性。

(2) BMA 安全策略主要原则。

① 访问控制表。每一份病历记录都有一个访问控制表标记,用以说明可以读取和添加数据的人和组。

② 打开记录。医生可以打开访问控制列表中与他有关的病人的病历。需要经过病人委托。

③ 控制。在每个访问控制列表中必须有一个是可信的,只有他才能对病历进行写入。

④ 同意和通报。可靠的医生在打开病历时,应将访问控制列表中的名字、后续条件、可靠性的传递通知病人。

⑤ 持续性。任何人都不能删除病历记录,除非它已过期。

⑥ 日志。记录对病历记录的全部访问。

⑦ 可信计算。处理以上原理的计算机应该有一个有效的方法实现,实现方法需要由独立专家评估。

5. 自主访问控制

自主型访问控制基于用户的身份和访问控制规则。自主保护策略管理用户的存取,这些信息是以用户的身份和授权为基础的,它们详细说明了对于系统中的每一个用户(或用户组)和每一个客体,允许用户对客体的存取模式(如读、写或执行)。根据指定的授权,用户存取客体的每一个要求都被检查。如果存在授权状态,则用户可以按指定的模式存取客体,存取被同意;否则被拒绝。DAC 之所以被称为自主的,是因为它允许用户将其访问权力赋予其他的用户。而且对于一个客体的否定授权高于对同一客体的肯定授权。自主策略的灵活性使它们适合于多种系统和应用。由于这些原因,在多种执行中,自主策略被广泛地应用,尤其在商业的和工业的环境中。自主访问控制的实现主要有 3 种方式:访问控制表(ACL);访问能力表(Capability);授权关系表。综合以上 3 种存取控制方法的优、缺点,访问控制表的方法以其在权限的授予和回收方面的高效率,在商业软件中得到了广泛应用。

自主访问控制特点:根据主体的身份和授权来决定访问模式。与 MAC 相比:松耦合,

分布式授权。缺点是信息在移动过程中，其访问权限关系会被改变。实现机制：访问控制列表 ACL(s,o)；权能列表 Capabilities(s,s)。

6. CC 安全技术模型

CC 是当前信息安全的最新国际标准，它是在 TESEC、ITSEC、CTCPEC、FC 等信息安全标准的基础上综合形成的。1993 年 6 月，美国政府同加拿大及欧共体共同起草单一的通用准则(CC 标准)，并将其推广到国际标准。制定 CC 标准的目的是建立一个各国都能接受的通用的信息安全产品和系统的安全性评估准则。

CC 定义了一套能满足各种需求的 IT 安全准则，共分为三部分：第一部分，简介和一般模型；第二部分，安全功能要求；第三部分，安全保证要求。其中心内容是：当在 PP(安全保护框架)和 ST(安全目标)中描述 TOE(评测对象)的安全要求时，应尽可能使其与第二部分描述的安全功能组件和第三部分描述的安全保证组件相一致。

CC 在第一部分描述了对安全保护框架(PP)和安全目标(ST)的要求。与传统的软件系统设计相比较，PP 实际上就是安全需求的完整表示，ST 则是通常所说的安全方案。CC 在第二部分和第三部分，分别详细介绍了为实现 PP 和 ST 所需要的安全功能要求和安全保证要求，并对安全保证要求进行了等级划分(共分为 7 个等级)。对于安全功能要求，CC 虽然没有进行明确的等级划分，但是在对每一类功能进行具体描述时，要求上还是有差别的。

CC 标准是目前国际通行的信息技术产品安全性评价规范，它基于保护轮廓和安全目标提出安全需求，具有灵活性和合理性，基于功能要求和保证要求进行安全评估，能够实现分级评估目标，不仅考虑了保密性评估要求，还考虑了完整性和可用性多方面安全要求。

7. 安全技术模型 ISO 7498-2

OSI(Open System Interconnection)模型，即开放式通信系统互联参考模型(Open Systems Interconnection Reference Model，OSI/RM)，是国际标准化组织(ISO)提出的一个试图使各种计算机在世界范围内互联为网络的标准框架，简称 OSI。

OSI 七层模型是一种框架型的设计方法，建立 7 层模型的主要目的是为解决异种网络互联时所遇到的兼容性问题，其最主要的功能就是帮助不同类型的主机实现数据传输。它的最大优点是将服务、接口和协议这 3 个概念明确地区分开来，通过 7 个层次化的结构模型使不同的系统不同的网络之间实现可靠的通信。

在制定计算机网络标准方面，起着重大作用的两大国际组织，即国际电报与电话咨询委员会(CCITT)、国际标准化组织(ISO)，虽然它们工作领域不同，但随着科学技术的发展，通信与信息处理之间的界限开始变得比较模糊，这也成了 CCITT 和 ISO 共同关心的领域。1974 年，ISO 发布了著名的 ISO/IEC 7498 标准，它定义了网络互联的 7 层框架，也就是开放式系统互联参考模型。1983 年正式批准使用。

在 ISO 7498-2 中描述了开放系统互联安全的体系结构，提出设计安全的信息系统的基础架构中应该包含 5 种安全服务(安全功能)，能够对这 5 种安全服务提供支持的 8 类安全机制和普遍安全机制，以及需要进行的 5 种 OSI 安全管理方式。安全技术模型结构如图 8.4 所示。

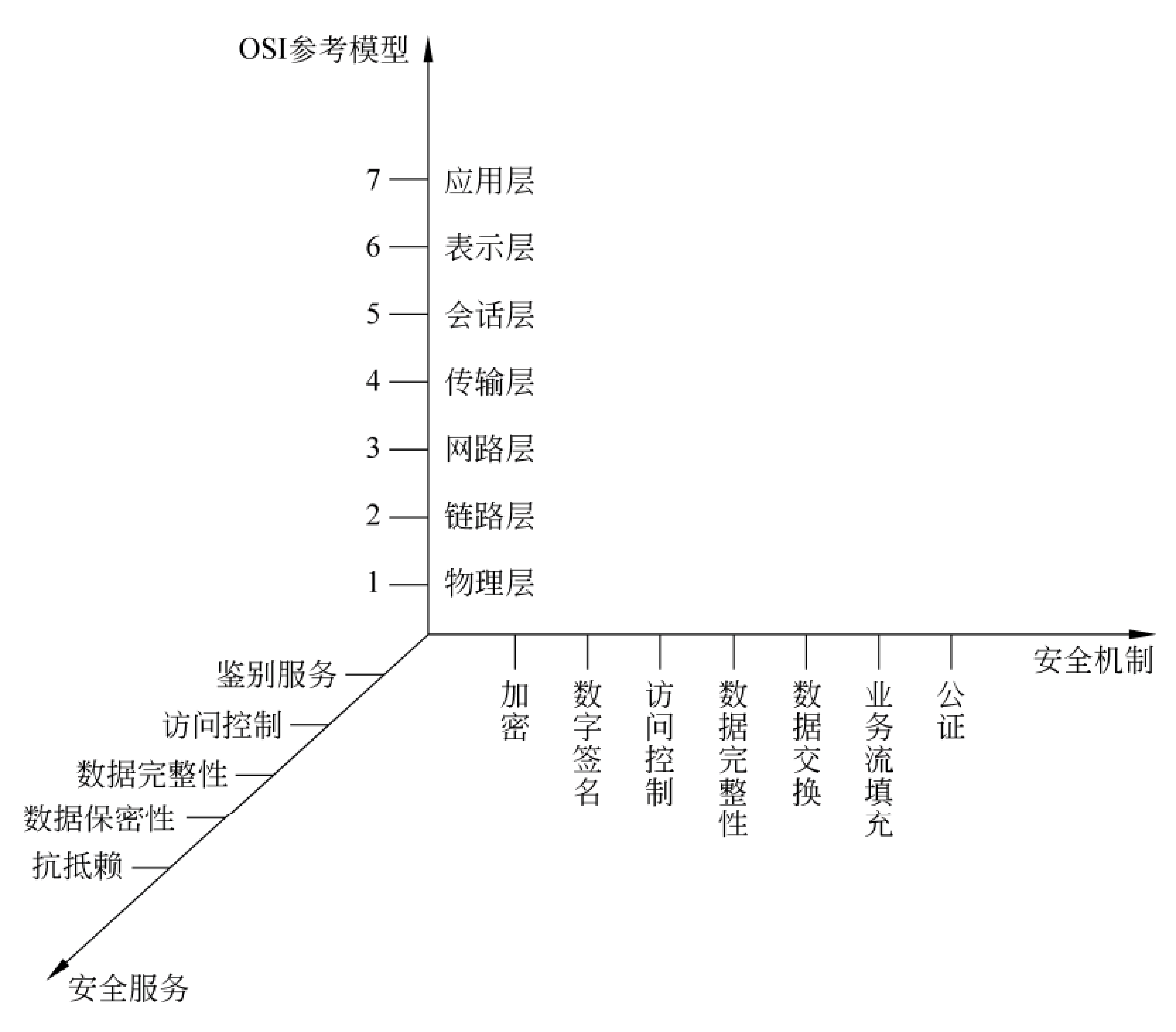


图 8.4 安全技术模型结构

8.3.3 信息系统安全问题产生的根源

1. 信息系统安全问题概述

根据信息系统安全的整体结构来看，信息系统安全可从 5 个层面，即物理、网络、主机系统、应用系统和数据对系统进行保护，因此，技术类安全要求也相应地分为 5 个层面上的安全要求。

（1）物理层面安全要求。主要是从外界环境、基础设施、运行硬件、介质等方面为信息系统的安全运行提供基本的后台支持和保证。

（2）网络层面安全要求。为信息系统能够在安全的网络环境中运行提供支持，确保网络系统安全运行，提供有效的网络服务。

（3）主机层面安全要求。在物理、网络层面安全的情况下，提供安全的操作系统和安全的数据库管理系统，以实现操作系统和数据库管理系统的安全运行。

（4）应用层面安全要求。在物理、网络、系统等层面安全的支持下，实现用户安全需求所确定的安全目标。

（5）数据及备份恢复层面安全要求。全面关注信息系统中存储、传输、处理等过程的数据的安全性。

2. 物理安全

物理安全保护的目的主要是使存放计算机、网络设备的机房以及信息系统的设备和存储数据的介质等免受物理环境、自然灾难以及人为操作失误和恶意操作等各种威胁所产生的攻击。物理安全是防护信息系统安全的最底层，缺乏物理安全，其他任何安全措施都是毫

无意义的。

物理安全主要涉及的方面包括环境安全(防火、防水、防雷击等)、设备和介质的防盗窃防破坏等方面。具体包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等 10 个方面。

3. 网络安全

网络安全为信息系统在网络环境的安全运行提供支持。一方面,确保网络设备的安全运行,提供有效的网络服务;另一方面,确保在网上传输数据的保密性、完整性和可用性等。由于网络环境是抵御外部攻击的第一道防线,因此必须进行各方面的防护。对网络安全的保护,主要关注两个方面:共享和安全。开放的网络环境便利了各种资源之间的流动、共享,但同时也打开了“罪恶”的大门。因此,必须在二者之间寻找恰当的平衡点,使得在尽可能安全的情况下实现最大程度的资源共享,这是实现网络安全的理想目标。

网络安全主要关注的方面包括网络结构、网络边界以及网络设备自身安全等,具体的方面包括结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护等 7 个方面。

4. 主机安全

主机系统安全是包括服务器、终端/工作站等在内的计算机设备在操作系统及数据库系统层面的安全。终端/工作站是带外设的台式机与笔记本计算机,服务器则包括应用程序、网络、Web、文件与通信等服务器。主机系统是构成信息系统的主要部分,其上承载着各种应用。因此,主机系统安全是保护信息系统安全的中坚力量。

5. 应用安全

通过网络、主机系统的安全防护,最终应用安全成为信息系统整体防御的最后一道防线。在应用层面运行着信息系统的基于网络的应用以及特定业务应用。基于网络的应用是形成其他应用的基础,包括消息发送、Web 浏览等,可以说是基本的应用。业务应用采纳基本应用的功能以满足特定业务的要求,如电子商务、电子政务等。由于各种基本应用最终是为业务应用服务的,因此对应用系统的安全保护最终就是如何保护系统的各种业务应用程序安全运行。

6. 数据安全及备份恢复

信息系统处理的各种数据(用户数据、系统数据、业务数据等)在维持系统正常运行上起着至关重要的作用。一旦数据遭到破坏(泄露、修改、毁坏),都会在不同程度上造成影响,从而危害到系统的正常运行。由于信息系统的各个层面(网络、主机、应用等)都对各类数据进行传输、存储和处理等,因此,对数据的保护需要物理环境、网络、数据库和操作系统、应用程序等提供支持。各个“关口”把好了,数据本身再具有一些防御和修复手段,必然将对数据造成的损害降至最小。另外,数据备份也是防止数据被破坏后无法恢复的重要手段,而硬件备份等更是保证系统可用的重要内容,在高级别的信息系统中采用异地适时备份会有效地防治灾难发生时可能造成的系统危害。保证数据安全和备份恢复主要从数据完整性、数据保密性、备份和恢复等 3 个方面来考虑。

“防患于未然”,即使对数据进行了种种保护,但仍无法绝对保证数据的安全。对数据进行备份,是防止数据遭到破坏后无法使用的最好方法。通过对数据采取不同的备份方式、备份形式等,保证系统重要数据在发生破坏后能够恢复。硬件的不可用同样也是造成系统无

法正常运行的主要原因。因此，有必要将一些重要的设备（服务器、网络设备）设置冗余。当主设备不可用时，及时切换到备用设备上，从而保证了系统的正常运行。如果有能力的话，对重要的系统也可实施备用系统，主应用系统和备用系统之间能实现平稳、及时的切换。

7. 安全管理制度

在信息安全中，最活跃的因素是人，对人的管理包括法律、法规与政策的约束、安全指南的帮助、安全意识的提高、安全技能的培训、人力资源管理措施及企业文化的熏陶，这些功能的实现都是以完备的安全管理政策和制度为前提。这里所说的安全管理制度包括信息安全工作的总体方针、策略、规范各种安全管理活动的管理制度以及管理人员或操作人员日常操作的操作规程。

8. 关于应急预案管理

相比于其他机构和领域，信息系统更容易受到各种安全事件和灾难的伤害而导致中断，特别是在一些突发情况下，如不采取应急响应，将会导致重大的社会影响、经济损失。于是建立有效的应急预案、灾难恢复计划并履行，对于削减系统损失与降低各种服务的不可用性就显得非常重要。

8.3.4 信息系统安全问题的威胁

信息化进程在加快，信息化的覆盖面在扩大，信息安全问题也就随之日益增多和复杂，其造成的影响和后果也会不断扩大和更趋严重。网络信息系统是一个复杂的计算机系统，它在物理上、操作上和管理上的种种漏洞导致系统安全十分脆弱。而信息又主要依托网络信息系统，这给信息安全带来新的问题和挑战。

信息安全面临的威胁主要来自以下 3 个方面。

1. 技术安全风险因素

（1）基础信息网络和重要信息系统安全防护能力不强。

国家重要的信息系统和信息基础网络是信息安全防护的重点，是社会发展的基础。我国的基础网络主要包括互联网、电信网、广播电视网，重要的信息系统包括铁路、政府、银行、证券、电力、民航、石油等关系国计民生的国家关键基础设施所依赖的信息系统。虽然在这些领域的信息安全防护工作取得了一定的成绩，但是安全防护能力仍然不强。主要表现在以下几点。

① 重视不够，投入不足。对信息安全基础设施投入不够，信息安全基础设施缺乏有效的维护和保养制度，设计与建设不同步。

② 安全体系不完善，整体安全还十分脆弱。

③ 关键领域缺乏自主产品，高端产品严重依赖国外，无形中埋下了安全隐患。我国计算机产品大都是国外的品牌，技术上受制于人，如果被人预先植入后门，很难发现，届时造成的损失将无法估量。

（2）失泄密隐患严重。

随着企业及个人数据累计量的增加，数据丢失所造成的损失已经无法计量，机密性、完整性和可用性均可能随时受到威胁。在当今全球一体化的大背景下，窃密与反窃密的斗争愈演愈烈，特别在信息安全领域，保密工作面临新的问题越来越多，越来越复杂。信息时代泄密途径日益增多，如互联网泄密、手机泄密、电磁波泄密、移动存储介质泄密等新的技术发

展也给信息安全带来新的挑战。

2. 人为恶意攻击

相对物理实体和硬件系统及自然灾害而言，精心设计的人为攻击威胁最大。人的因素最为复杂，思想最为活跃，不能用静止的方法和法律、法规加以防护，这是信息安全所面临的最大威胁。人为恶意攻击可以分为主动攻击和被动攻击。主动攻击的目的在于篡改系统中信息的内容，以各种方式破坏信息的有效性和完整性。被动攻击的目的是在不影响网络正常使用的情况下，进行信息的截获和窃取。总之，不管是主动攻击还是被动攻击，都给信息安全带来巨大损失。攻击者常用的攻击手段有木马、黑客后门、网页脚本、垃圾邮件等。

3. 信息安全管理薄弱

面对复杂、严峻的信息安全管理形势，根据信息安全风险的来源和层次，有针对性地采取技术、管理和法律等措施，谋求构建立体的、全面的信息安全管理体系，已逐渐成为共识。与反恐、环保、粮食安全等安全问题一样，信息安全也呈现出全球性、突发性、扩散性等特点。信息及网络技术的全球性、互联性、信息资源和数据共享性等，又使其本身极易受到攻击，攻击的不可预测性、危害的连锁扩散性大大增强了信息安全问题造成的危害。信息安全管理已经被越来越多的国家所重视。与发达国家相比，我国的信息安全管理研究起步比较晚，基础性研究较为薄弱。研究的核心仅仅停留在信息安全法规的出台，信息安全风险评估标准的制定及一些信息安全管理的实施细则，应用性研究、前沿性研究不强。这些研究没有从根本上改变我国管理底子薄、漏洞多的现状。

但这些威胁根据其性质，基本上可以归结为以下几个方面：

（1）信息泄露。保护的信息被泄露或透露给某个非授权的实体。

（2）破坏信息的完整性。数据被非授权地进行增删、修改或破坏而受到损失。

（3）拒绝服务。信息使用者对信息或其他资源的合法访问被无条件地阻止。

（4）非法使用(非授权访问)。某一资源被某个非授权的人，或以非授权的方式使用。

（5）窃听。用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。例如，对通信线路中传输的信号搭线监听，或者利用通信设备在工作过程中产生的电磁泄露截取有用信息等。

（6）业务流分析。通过对系统进行长期监听，利用统计分析方法对如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

（7）假冒。通过欺骗通信系统或用户，达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的目的。平常所说的黑客大多采用的就是假冒攻击。

（8）旁路控制。攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。例如，攻击者通过各种攻击手段发现原本应保密，但是却又暴露出来的一些系统“特性”，利用这些“特性”，攻击者可以绕过防线守卫者侵入系统的内部。

（9）授权侵犯。被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他非授权的目的，也称为“内部攻击”。

（10）抵赖。这是一种来自用户的攻击，涵盖范围比较广泛，如否认自己曾经发布过的某条消息、伪造一份对方来信等。

（11）计算机病毒。这是一种在计算机系统运行过程中能够实现传染和侵害功能的程序，行为类似病毒，故称为计算机病毒。

（12）信息安全法律法规不完善，由于当前约束操作信息行为的法律法规还很不完善，存在很多漏洞，很多人打法律的擦边球，这就给信息窃取、信息破坏者以可乘之机。

8.3.5 信息安全保障评估框架的组成

信息安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，在中国、美国等很多国家都存在的一种信息安全领域的工作。在中国，信息安全等级保护广义上为涉及该工作的标准、产品、系统、信息等均依据等级保护思想的安全工作；狭义上，一般指信息系统安全等级保护，是指对国家安全、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置的综合性工作。

1. 信息系统安全保障等级评估保障的内容和对象

信息安全等级保护工作包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查5个阶段，作为公安部授权的第三方测评机构，为企事业单位提供免费专业的信息安全等级测评咨询服务。

信息系统安全保障的对象：技术目标；服务目标；管理目标；人员目标；政策、需求目标。

2. 信息系统安全保障要求（ISPP）

信息系统保护轮廓（ISPP）是根据组织机构使命和所处的运行环境，从组织机构的策略和风险的实际情况出发，对具体信息系统安全保障需求和能力进行具体描述。表达一类产品或系统的安全目的和要求。ISPP是从信息系统的所有者（用户）的角度规范化、结构化地描述信息系统安全保障需求。

3. 信息系统安全保障目标（ISST）

信息系统安全目标（ISST）是根据信息系统保护轮廓（ISPP）编制的信息系统安全保障方案。某一特定产品或系统的安全需求。ISST从信息系统安全保障的建设方（厂商）的角度制定的信息系统安全保障方案。

4. 技术保障

（1）安全技术架构相关含义。安全技术体系是对组织机构信息技术系统的安全体系结构的整体描述。安全技术架构能力是拥有信息技术系统的组织机构根据其策略的要求和风险评估的结果，参考相关技术体系构架的标准和最佳实践，结合组织机构信息技术系统的具体现状和需求，建立的符合组织机构信息技术系统战略发展规划的信息技术系统整体体系框架；它是组织机构信息技术系统战略管理的具体体现。技术架构能力是组织机构执行安全技术整体能力的反映，它反映了组织机构在执行信息安全技术体系框架管理达到预定的成本、功能和质量目标上的度量。

（2）安全架构能力成熟度级别。

能力级别0：未实施。

能力级别1：非规范化设计、基本执行级。

能力级别2：文档化设计、规范定义级。

能力级别3：结构化设计、正式执行级。

能力级别4：半形式化设计、测试验证级。

能力级别5：形式化设计、审计优化级。

(3) 技术组件分类。

FAU类：安全审计。

FCO类：通信。

FCS类：密码支持。

FDP类：用户数据保护。

FIA类：标识和鉴别。

FMT类：安全管理。

FPR类：隐私。

FPT类：TSF保护。

FRU类：资源利用。

FTA类：TOE访问。

FTP类：可信路径/信道。

5. 管理保障

(1) ITIL即IT基础架构库由英国政府部门在20世纪80年代末制订，现由英国商务部负责管理，主要适用于IT服务管理(ITSM)。ITIL为企业的IT服务管理实践提供了一个客观、严谨、可量化的标准和规范。

(2) COBIT(Control Objectives for Information and related Technology)是目前国际上通用的信息系统审计的标准，由信息系统审计与控制协会在1996年公布。这是一个在国际上公认的、权威的安全与信息技术管理和控制的标准，目前已经更新至5.0版。它在商业风险、控制需要和技术问题之间架起了一座桥梁，以满足管理的多方面需要。该标准体系已在世界100多个国家的重要组织与企业中运用，指导这些组织有效利用信息资源，有效地管理与信息相关的风险。

(3) 美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)直属美国商务部，从事物理、生物和工程方面的基础和应用研究，以及测量技术和测试方法方面的研究，提供标准、标准参考数据及有关服务，在国际上享有很高的声誉。

(4) 英国标准协会(BSI)成立于1901年，当时称为英国工程标准委员会。经过100多年的发展，现已成为举世闻名的集标准研发、标准技术信息提供、产品测试、体系认证和商检服务五大互补性业务于一体的国际标准服务提供商，面向全球提供服务。BSI目前在世界110个国家和地区设有办事处或办公室，拥有员工5500人，其中75%在国外。作为全球权威的标准研发和国际认证评审服务提供商，BSI倡导制定了世界上流行的ISO 9000系列管理标准，在全球多个国家拥有注册客户，注册标准涵盖质量、环境、健康和安全、信息安全、电信和食品安全等几乎所有领域。

(5) 经济合作与发展组织(OECD)，是由30多个市场经济国家组成的政府间国际经济组织，旨在共同应对全球化带来的经济、社会和政府治理等方面的挑战，并把握全球化带来的机遇。成立于1961年，目前成员国总数为34个，总部设在巴黎。

6. 工程保障

安全工程过程生命周期：

(1) 挖掘安全需求。本阶段建立项目组织，了解系统的上下文环境，决定开始进行安全

工程,制定初步计划和预算等。

本阶段信息系统安全工程师帮助用户挖掘并理解完成系统的任务和业务所需的信息保护需求。信息保护需求的确定建立在对系统的安全风险分析的基础上。

(2) 定义安全需求。本阶段信息系统工程师将已识别出来的信息保护需求落实到各子系统中,包括开发系统安全上下文、初步的系统安全运行设想和安全要求基线等。相关过程域:系统定义(PEN_SDF)、评估威胁(PRM_ATT)、评估脆弱性(PRM_AVL)、评估影响(PRM_AIM)、评估安全风险(PRM_ASR)、确定安全要求(PEN_ISR)。

(3) 设计体系结构。本阶段信息系统安全工程师与系统工程师一起进行分析候选体系结构、分配安全服务和选择安全机制,从而完成安全功能分析和落实。信息系统安全工程师选择适用的组件或元件,并把安全功能分配给这些元件,同时描述这些元件之间的关系。

(4) 详细安全设计。本阶段信息系统安全工程师分析设计的约束条件,分析折中办法,进行详细的系统和安全设计并考虑生命周期支持。信息系统安全工程师检查所有系统安全需求落实到了组件。最终的详细安全设计结果为实现系统提供充分的组件和接口描述信息。相关过程域:提供安全输入(PEN_PSI)、高层安全设计(PEN_HSD)、详细安全设计(PEN_DSD)。

(5) 实现系统安全。本阶段信息系统安全工程师把系统设计转移到运行,参与对所有系统问题的多学科综合分析,并为认证认可活动提供输入。例如,验证系统已经实现了对抗威胁评估中识别出的威胁;追踪与系统实现和测试活动相关的信息保护保障机制;为系统生命周期支持计划、运行规程、培训材料维护提供输入。本阶段信息系统已到位并开始运行,通过定期的评估和不断监视系统的安全状况,确定如何获得更高的安全性能和效率等来满足用户变化的安全需求,进行软硬件升级和修改并进行相应的测试。相关过程域:安全工程实施(PEN_SEE)、协调安全(PEN_COS)、监视安全态势(PEN_MSP)、管理安全控制(PEN_MSC)。

(6) 有效性评估。本阶段信息系统安全工程师关注信息保护的有效性——系统是否能够保证其处理信息的保密性、完整性、可用性、鉴别和不可否认性,确保成功完成使命。相关过程域:验证和确认安全(PAS_VVS)、建立保障论据(PAS_EAE)。

8.4 信息系统安全保障建设和评估实践

8.4.1 信息系统安全保障建设和评估实施

1. 确定信息系统安全保障需求

任务1:确定信息系统安全保障能力级。

(1) TCML 安全技术架构能力级。

(2) MCML 安全管理能力级。

(3) ECML 安全过程能力级。

任务2:确定信息系统的具体安全保障需求:通过风险评估、需求分析等来对信息系统安全保障需求进行描述。

提取信息安全需求的必要性:信息安全需求是安全方案设计和安全措施实施的依据。

准确地提取安全需求，一方面可以保证安全措施可以全面覆盖信息系统面临的风险，是安全防护能力达到业务目标和法规政策要求的基础；另一方面可以提高安全措施的针对性，避免不必要的安全投入，防止浪费。

2. 规范化、结构化描述信息系统安全保障具体需求

信息系统安全保障的具体需求由信息系统保护轮廓(ISPP)确定。

任务3：编制信息系统安全保障要求(ISPP)。

安全保障目的对安全环境的符合性，安全保障要求对安全保障目的的符合性。

安全目的提供预期响应安全需求的简要陈述，既有由TOE满足的安全目的，也有由TOE环境中IT的或非IT的方法满足的安全目的。《信息技术安全性评估准则》(GB/T 18336)建议，安全目的不应涉及决定安全需求解决方法的实现细节。

TOE安全环境定义TOE预期处理的“安全需求”，指明安全问题(环境的假设、已知的威胁、TOE必须使用的组织安全策略)，部分作用是形成安全需求。

3. 根据信息系统安全保障需求编制具体的安全保障解决方案

(1) 信息安全保障解决方案是一个动态的风险管理过程，通过对信息系统生命周期内风险的控制，来解决在运行环境中信息系统安全建设所面临的各种问题，从而有效保障业务系统及应用的持续发展。

(2) 信息安全保障解决方案制定的原则。以风险评估和法规要求得出的安全需求为依据，考虑系统的业务功能和价值，考虑系统风险哪些是必须处置的，哪些是可接受的。贴合实际具有可实施性，可接受的成本，合理的进度，技术可实现性，组织管理和文化的可接受性。

(3) 规范化、结构化信息系统安全保障方案。根据信息系统保护轮廓(ISPP)编制的信息系统安全保障方案，来制定信息系统安全目标(ISST)。信息系统安全目标中，评估对象应包括信息系统整体、信息系统安全管理、信息系统安全技术、信息系统安全工程；标准中所描述的信息系统安全目标是将信息系统整体作为评估对象，在应用于安全管理保障、安全技术和信息系统安全工程这些方面的评估时，可对部分内容进行裁减。

任务4：编制信息系统安全保障目标：包括控制要求和能力成熟度要求。

技术保障要求来自于支持信息系统安全保障的那些技术领域中期望的安全行为。

管理保障要求来自于支持信息系统安全保障的那些管理领域中期望的安全行为。

工程保障要求来自于支持信息系统安全保障的那些工程领域中期望的安全行为。

通过合理选择的安全技术保障、管理和工程保障控制要求及其能力成熟度级，可以确保达到一定的安全保障目的。

(4) 信息安全保障实施的原则。以信息安全保障方案为依据，覆盖方案提出的建设目标和建设内容。规范的实施过程：实施的质量、进度和成本必须受控，实施过程中出现的变更必须受控，充分考虑实施风险，如资源不足、组织文化的抵触情绪、对业务正常运行造成的影响、信息泄露或破坏等。

(5) 信息安全保障实施的内容。覆盖信息系统全生命周期，以风险和策略为核心，风险评估贯穿系统全生命周期，建立完整的策略体系。涉及技术、管理、工程、人。

技术：分层多点的深度防御系统。

管理：建立能力成熟的信息安全管理体系。

工程：选择有能力的信息安全集成商和服务商。

人：建立完善的人才体系，增强安全意识和文化。

(6) 信息安全保障实施——管理体系建设。使命要求；组织体系建设；策略体系(风险管理、业务持续性管理、应急响应管理、意识培训和教育)；系统测评、风险评估；生命周期安全管理。

(7) 信息安全人才体系战略组织机构信息安全人才体系战略。对组织机构来说，应建立一个完整的信息安全人才体系，信息安全人才体系应包括所有员工，需要进行信息安全保障意识教育，具体可以使用各种海报、组织机构网站上发布相关信息等以增强所有员工的安全意识；对于涉及信息系统的岗位和职责的员工而言，需要进行相应的信息安全保障培训；注册信息安全员(CISM)为这些员工提供了全面的信息安全保障基础知识；对于信息安全专业人员而言，应建立更全面、专业的信息安全保障知识和经验；注册信息安全专业人员(CISP)为这些人员提供了信息安全专业知识能力的证明。

4. 信息系统安全保障评估

信息系统安全保障评估——在信息系统所处的运行环境中对信息系统安全保障的具体工作和活动进行客观的评估，通过信息系统安全保障评估所搜集的客观证据，向信息系统的所有相关方提供信息系统的安全保障工作能够实现其安全保障策略，能够将其所面临的风险降低到其可接受程度的主观信心。评估是信息系统安全保障的一个重要概念，系统所有者可以根据评估所得到的客观评估结果建立其主观的信心。评估对象是信息系统，不仅包含了信息技术系统，还包括同信息系统所处的运行环境相关的人和管理等领域。

1) 国外信息安全保障测评

信息系统安全保障评估主要包括两方面的评估：信息系统在其运行环境中具体的安全保障控制相对于安全保障要求的符合性的评估以及信息系统安全保障级的评估。

信息化发展比较好的发达国家，特别是美国，非常重视国家信息安全的管理工作。美国、俄罗斯、日本等国家都已经或正在制订自己的信息安全发展战略和发展计划，确保信息安全沿着正确的方向发展。美国信息安全管理的最高权力机构是美国国土安全局，分担信息安全管理和执行的机构有美国国家安全局、美国联邦调查局、美国国防部等，主要是根据相应的方针和政策结合自己部门的情况实施信息安全保障工作。2000 年初，美国出台了计算机空间安全计划，旨在加强关键基础设施、计算机系统网络免受威胁的防御能力。2000 年 7 月，日本信息技术战略本部及信息安全会议拟定了信息安全指导方针。2000 年 9 月，俄罗斯批准了《国家信息安全构想》，明确了保护信息安全的措施。

美国、俄罗斯、日本均以法律的形式规定和规范信息安全工作，对有效实施安全措施提供了有力保证。2000 年 10 月，美国的电子签名法案正式生效。2000 年 10 月，美国参议院通过了《互联网网络完备性及关键设备保护法案》。日本于 2000 年 6 月公布了旨在对付黑客的《信息网络安全可靠性基准》的补充修改方案。2000 年 9 月，俄罗斯实施了关于网络信息安全的法律。国际信息安全管理已步入标准化与系统化管理时代。在 20 世纪 90 年代之前，信息安全主要依靠安全技术手段与不成体系的管理规章来实现。随着 20 世纪 80 年代 ISO 9000 质量管理体系标准的出现及随后在全世界的推广应用，系统管理的思想在其他领域也被借鉴与采用，信息安全管理也同样在 20 世纪 90 年代步入了标准化与系统化的管理时代。1995 年英国率先推出了 BS7799 信息安全管理标准，该标准于 2000 年被国际标准化

组织认可为国际标准 ISO/IEC 17799。现在该标准已引起许多国家与地区的重视，在一些国家已经被推广与应用。组织贯彻实施该标准可以对信息安全风险进行安全系统的管理，从而实现组织信息安全。其他国家及组织也提出了很多与信息安全管理相关的标准。

2）国内信息安全现状

我国已初步建成了国家信息安全组织保障体系。国务院信息办专门成立了网络与信息安全领导小组，各省、市、自治州也设立了相应的管理机构。2003 年 7 月，国务院信息化领导小组通过了《关于加强信息安全保障工作的意见》，同年 9 月，中央办公厅、国务院办公厅转发了《国家信息化领导小组关于加强信息安全保障工作的意见》，把信息安全提到了促进经济发展、维护社会稳定、保障国家安全、加强精神文明建设的高度，并提出了"积极防御，综合防范"的信息安全管理方针。2003 年 7 月，成立了国家计算机网络应急技术处理协调中心，专门负责收集、汇总、核实、发布权威性的应急处理信息。2001 年 5 月，成立了中国信息安全产品测评认证中心和代表国家开展信息安全测评认证工作的职能机构，还建立了依据国家有关产品质量认证和信息安全管理的法律法规管理和运行国家信息安全测评认证体系。

我国制定和引进了一批重要的信息安全管理标准。发布了国家标准《计算机信息系统安全保护等级划分准则》(GB 17895—1999)、《信息系统安全等级保护基本要求》等技术标准和《信息安全技术信息系统安全管理要求》(GB/T 20269—2006)、《信息安全技术信息系统安全工程管理要求》(GB/T 20282—2006)、《信息系统安全等级保护基本要求》等管理规范，并引进了国际上著名的《ISO 17799：2000：信息安全管理实施准则》、《BS 7799—2：2000：信息安全管理体系实施规范》等信息安全管理标准。

从 20 世纪 90 年代初起，为配合信息安全管理的需要，国家相关部门、行业和地方政府相继制定了《中华人民共和国计算机信息网络国际联网管理暂行规定》、《商用密码管理条例》、《互联网信息服务管理办法》、《计算机信息网络国际联网安全保护管理办法》、《电子签名法》等有关信息安全管理的法律法规文件。

信息安全风险评估工作已经开展，并成为信息安全管理的核心工作之一，由国家信息中心组织先后对 4 个地区(北京、广州、深圳和上海)，十几个行业的 50 多家单位进行了深入细致的调查与研究，最终形成了《信息安全风险评估调查报告》、《信息安全风险评估研究报告》和《关于加强信息安全风险评估工作的建议》，制定了《信息安全技术信息安全风险评估规范》(GB/T 20984—2007)。

3）我国信息安全管理存在的问题

信息安全管理现状比较混乱，缺乏一个国家层面上的整体策略，实际管理力度不够，政策执行和监督力度也不够；具有我国特点的、动态的和涵盖组织机构、文件、控制措施、操作过程和程序及相关资源等要素的信息安全管理体系还未建立起来；具有我国特点的信息安全风险评估标准体系还有待完善，信息安全的需求难以确定，缺乏系统、全面的信息安全风险评估和评价体系以及全面、完善的信息安全保障体系；信息安全意识缺乏，普遍存在重产品、轻服务，重技术、轻管理的思想；专项经费投入不足，管理人才极度缺乏，基础理论研究和关键技术薄弱，严重依靠国外；技术创新不够，信息安全管理产品水平和质量不高；缺乏权威、统一、专门的组织、规划、管理和实施协调的立法管理机构，致使我国现有的一些信息安全管理方面的法律法规层次不高，执法主体不明确，多头管理，规则冲突，缺乏可操作性，执

行难度较大，有法难依。

4）国家信息安全测评

信息产品安全评估是测评机构对产品的安全性作出的独立评价，目的是为产品认证提供证据，增强用户对已评估产品安全的信任，向消费者提供信息技术安全产品的采购依据，从而推动信息技术安全产业的发展，提高信息技术安全科研和生产水平。信息产品安全测评依据的标准是CC、CEM和CNITSEC的要求。信息系统安全测评标准是《信息系统安全保障评估框架》(GB/T 20274)，它为信息系统安全测评提供了思路框架和操作规范。根据国家标准《信息技术安全性评估准则》(GB/T 18336—2001)，信息产品安全的测评由低到高划分为7个级别，即CC的EAL1～7级。目前中国信息安全测评中心开展了1～4级4个级别的测评工作。5～7级3个级别的测评将视具体情况与委托方研究协商后确定。获得的级别越高，安全性与可信度越高。信息产品安全测评流程有4个阶段，分别是准备阶段、评估阶段、认证阶段、监督和维持阶段。

5）信息系统安全保障评估

信息系统安全保障的评估，是从信息系统安全保障的概念出发，在信息系统的生命周期内，根据组织机构的要求在信息系统的安全技术、安全管理和安全工程领域内对信息系统的安全技术控制措施和技术架构能力、安全管理控制和管理能力以及安全工程实施控制措施和工程实施能力进行评估综合，从而最终得出信息系统在其运行环境中安全保障措施满足其安全保障要求的符合性以及信息系统安全保障能力的评估。评估信息系统安全保障目标对信息系统安全保障要求的符合性，即具体的信息系统安全保障措施信息系统在其运行环境下是否满足信息系统安全保障的需求。对信息系统安全保障的执行能力进行评估，评估信息系统安全保障级（包括技术架构能力级、工程能力级和管理能力级的评定）。信息系统安全保障的分级，需要先根据信息系统所处理信息的机密性、完整性和可用性特征以及信息和信息系统价值划分定义其使命类，然后考虑信息安全保障所要处理的威胁级别，最后再根据使命类和威胁级别的矩阵确定相对应的信息系统安全保障级（ISAL）要求。信息系统的安全保障能力成熟度等级有3个级别，分别是：管理能力成熟度等级（MCML），包括MCML1、MCML2、MCML3、MCML4和MCML5；工程能力成熟度等级（PCML），包括PCML1、PCML2、PCML3、PCML4和PCML5；技术体系架构成熟度级别（TCML），包括TCML1、TCML2、TCML3、TCML4、TCML5。具体而言，管理能力成熟度：一级表示组织内部能够依据经验进行部分的安全管理工作；二级表示组织能够建立完善的管理体系来规范安全管理管理能力；三级表示组织能够采取有效措施来敦促所制定管理体系的落实和实施；从而确保了管理体系有效地实施；四级表示组织所制定的管理体系不仅能够有效实施，而且还能够对实施的管理措施的效果进行测试，尽量采用量化的数据来分析和验证所采用的管理体系；五级表示组织能够对管理体系进行持续改进，使管理体系始终对组织安全保障体系的运行发挥最大效应。在基于安全风险分析得出的信息系统安全保护等级划分的基础上，提出安全需求，即得到评估对象的保护轮廓。参照评估准则和规范，制定出评估预案和规划，使用相应评估方法和工具，即可实施对评估对象的评估操作。评估中发现的问题、差距再反馈到评估的预案制订和安全需求，评估对象做相应调整、优化，达到信息系统资产所有者保证资产安全的初衷，即残余风险是可以承受的，资产价值受到保护，使命可以完成，最后得到评估结论，并给出安全等级的认证。为了提炼出评估对象的安全需求，需要建立安全

环境，综合考虑以下因素：需要保护的信息系统资产，系统所要完成的使命、组织管理、所处的物理环境，其面临的威胁、信息对抗的假设，然后在该特定的安全环境下确立系统的安全目标，提出系统的安全需求，包括安全技术需求、安全管理需求、安全过程需求和系统服务安全的需求，最终形成系统安全保障等级评估的规范(即系统保护轮廓和安全目标)。

6）服务商资质测评

信息安全服务是指信息安全工程的设计、实施、测试、运行和维护，以及相关的咨询和培训活动。信息安全服务资质测评是对信息安全服务商的技术、资源、管理等方面的能力和稳定性、可靠性进行评估。目前中国信息安全测评中心开展的信息安全服务资质评估包括3个类别：信息安全工程类、信息安全开发类、信息系统灾难恢复类。服务资质测评的作用是对安全服务提供方可以获得自身安全服务能力的认可，获得自身安全服务能力规范和提高(可重复、可预测的过程和实施减少返工)，还可以提高组织的市场竞争力(知名度)。对安全服务需求方可以获得选择服务商的第三方保证并提供有能力、有保障的服务商的范围(选择依据)。对社会和行业来说，可以规范和指导整个社会和信息安全服务行业的行为并搭建起信息安全服务领域科学的、规范的发展框架。安全工程过程能力级别是评定信息系统安全服务组织资质的主要依据，标志着服务组织提供给客户的安全服务专业水平和质量保证程度。信息系统工程的过程能力级别按成熟度排序，表示依次增加的组织能力。《信息系统安全服务资质评估准则》将信息系统安全服务组织的工程能力分为5个级别：一级，基本执行级；二级，计划跟踪级；三级，充分定义级；四级，量化控制级；五级，连续改进级。项目和组织过程能力包括：质量保证；管理配置；管理项目风险；监控技术活动；规划技术活动；管理系统工程支持环境；提供不断发展的技能和知识；与供应商协调。

7）信息安全人员资质测评

注册信息安全专业人员(Certified Information Security Engineer，CISP)是一种特殊专业岗位人员，其所具备的专业资质和能力，系经国家认证和认可。CISP的基本职能是对信息系统的安全提供技术保障。申请CISP认证的境内人员必须具备相关的教育和工作经历，通过信息安全专业人员培训及考试，提交申请，并由认证中心认证。CISP证书在有效期内实行年度确认制度，在有效期结束进行复查换证。CISP是主要从事信息安全技术开发服务工程建设等工作，CISO从事信息安全管理等相关工作，CISA从事信息系统的安全性审核或评估等工作。CISP可根据实际岗位工作需要，分为两个基础类别，即：注册信息安全工程师Certified Information Security Engineer(CISE)，适合从事信息安全技术领域的工作；注册信息安全管理人员(Certified Information Security Officer，CISO)，适合信息安全管理领域的工作；在两个基础类别之上还有两个扩展类别：注册信息安全专业人员—审计师(Certified Information Security Auditor，CISP-AUIT(原CISA))，适合从事信息安全审计工作；注册信息安全专业人员—灾难恢复工程师(CISP-DRP)，适合从事信息系统灾难恢复工作。CISP的知识体系架构主要由安全体系模型(信息安全保障框架、信息安全测试评估、计算机架构)与安全模型构成。

任务5：评估信息系统安全保障目标对信息系统安全保障要求的符合性，即具体的信息系统安全保障措施信息系统在其运行环境下是否满足信息系统安全保障的需求。

任务6：对信息系统安全保障的执行能力进行评估，评估信息系统安全保障级(包括技术架构能力级、工程能力级和管理能力级的评定)。

5. 根据评估结果持续改进

用户根据信息系统安全保障评估的结果进行改进，形成满足其信息系统安全保障需求的可持续改进的信息系统安全保障能力。信息系统安全保障需要覆盖信息系统的整个生命周期，形成持续改进的信息系统安全保障能力（技术/管理/工程能力）。

8.4.2 信息安全监控与维护

1. 系统安全监控维护的意义

系统安全主要是指硬件设备的安全，也包括应用软件与文档的安全及数据的安全。为保证系统中硬件的安全，应建立并严格执行有关制度，如进入机房的制度，禁止非机房值班人员随意进入机房；设备操作制度，禁止非值班人员操作机器；设备的保养维修制度，应定期、定时检查设备的运行状态，保证有足够的设备备件及备品，及时排除各种故障苗头。系统的工作是靠应用软件来实现的。故保证应用软件的安全十分重要。信息系统维护过程中必须加强对原版应用软件的管理，以备日后需要时进行复制。而在系统中运行工作的，是复制的应用软件。各种文档资料是保证系统有序工作及进行系统维护与日常运营管理的重要依据。因此，也应建立备份并妥善保管，应建立使用文档资料的制度并严格执行。为防止系统中数据资料的丢失、损坏及防止他人篡改、滥用系统内的数据信息，应利用加密技术及规定进入系统的权限，来保证系统中数据的安全。计算机系统一旦遭受破坏，将给使用单位造成重大经济损失，并严重影响正常工作的顺利开展。加强计算机系统安全工作，是信息化建设的重要工作内容之一。

2. 信息系统安全监控与保持

从风险的角度看，信息系统只有以下两种：一种是已经被攻破的；另一种是即将被攻破的。也就是说，没有一种信息系统是安全的。所以应该无时无刻地对信息系统进行监控，并且使系统保持在安全的状态下运行。

3. 信息系统安全监控与保持的工作内容

持续的风险评估是信息安全保障的一项基础性工作，新的安全决策和需求提供重要依据。以风险管理为基础做好以下工作：

（1）安全漏洞隐患的消控。

（2）建立有效事件管理与应急响应机制。

（3）建立强大的信息系统灾难恢复能力。

8.5 本章小结

信息保障是一种确保信息和信息系统能够安全运行的防护性行为。信息安全保障的“深度防御”就是要对攻击者和目标之间的信息环境构建连续的、层次化的多重防御机制，保障用户信息及信息系统的安全。信息安全保障体系主要是通过改善防御空间的同步效果、提高感知能力、加快响应速度、增强防御能力和生存能力等行为，从而提升系统整体的信息保障效能，是实施信息安全保障的法律法规、组织管理、安全技术和安全实施建设等方面有机结合的整体，是信息社会国家安全的基本组成部分，是保证国家信息化顺利进行的基础。实施信息安全保障是世界各国谋求的战略性制高点。重视信息安全保障工作，就是要将其作为信息安全的系统工程来看待。

第 9 章　信息安全标准介绍

导入语：本章介绍了安全标准化、信息安全评估标准、信息安全管理标准和等级保护标准四部分内容。安全标准化概述了信息安全标准化概况与信息安全标准化组织。信息安全评估标准介绍了安全技术评估标准发展历史，信息安全技术评估准则与信息系统安全保障评估框架。信息安全管理标准介绍了国际信息安全管理重要标准与我国信息安全管理重要标准。等级保护标准介绍了等级保护定级指南、等级保护基本要求与其他等级保护重要标准。本章主要知识结构如图 9.1 所示。

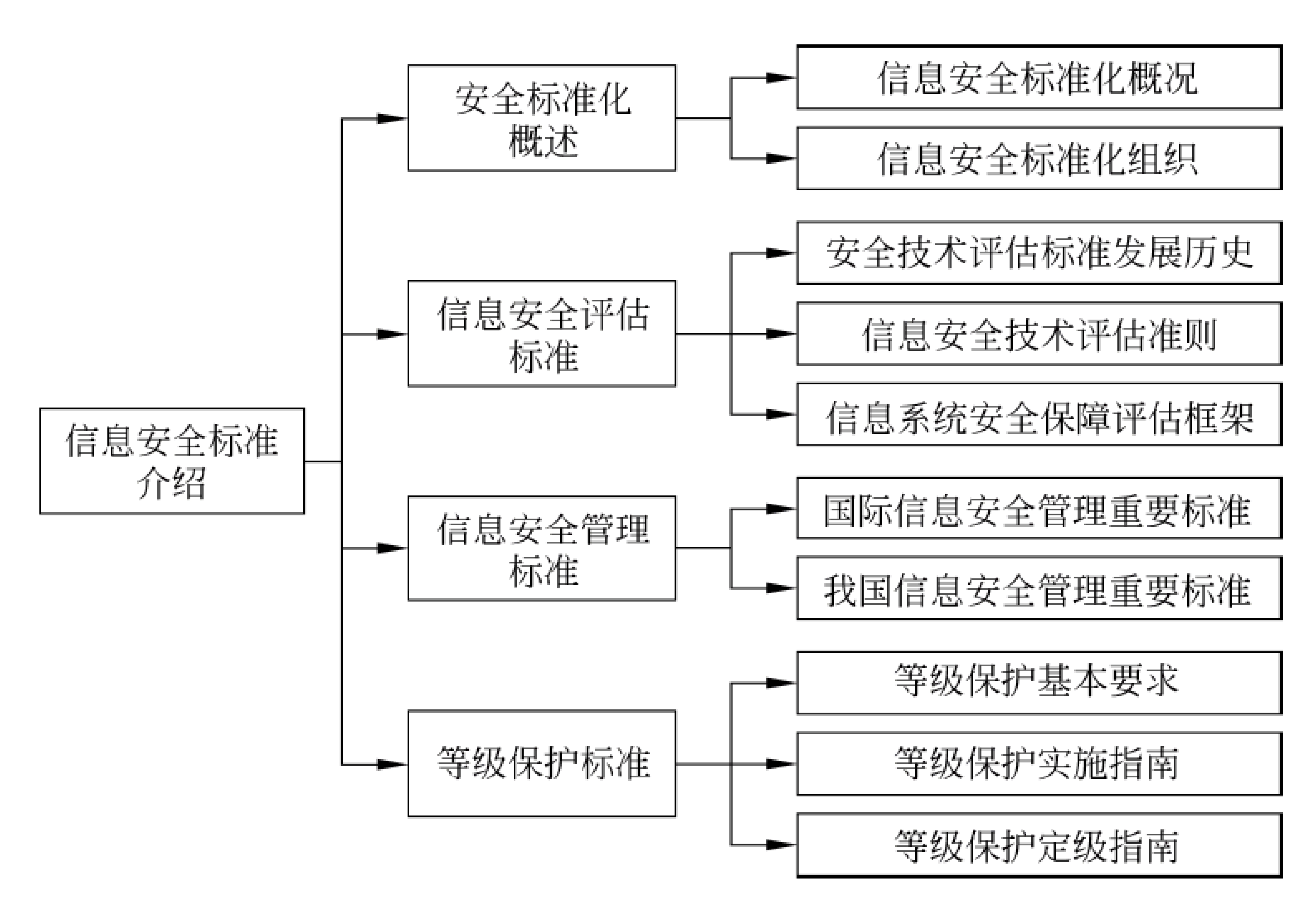


图 9.1　知识结构框图

考核目标：在安全标准化概述中，要了解标准和标准化的基本概念和作用、信息安全标准体系、国际信息安全标准化组织和我国信息安全标准化组织。在信息安全评估标准中，要了解安全技术评估标准发展过程，理解可信计算机评估准则（TCSEC）的局限性、《信息技术安全性评估准则》（GB/T 18336）（CC）的优点，了解 CC 的结构，理解 CC 的术语（TOE、PP、ST、EAL）和基本思想，了解使用 CC 进行信息技术产品安全性评估的基本过程，了解通用评估方法（CEM）；信息系统安全保证评估框架，了解《信息系统安全保障评估框架》（GB/T 20274）的目的和意义，了解《信息系统安全保障评估框架》（GB/T 20274）的结构和主要内容。在信息安全管理标准中，要了解国外信息安全管理标准发展概况，掌握 ISO 27001 和 ISO 27002 的主要内容，了解英国和美国等发达国家的信息安全管理标准，掌握《信息安全风险评估规范》（GB/T 20984）的主要内容，掌握《信息安全风险管理规范》（GB/Z 24364）的主要内容，了解《信息安全事件管理指南》（GB/Z 20985）的主要内容，掌握《信息安全事件分类分级指南》（GB/Z 20986）的主要内容，掌握《信息系统灾难恢复规范》（GB/T 20988）的主要内容。在等级保护标准部分中，要了解《信息系统安全保护等级定级指南》（GB/T 22240）的主要内容，掌握 5 个信息系统安全保护等级的定义；掌握系统定级的要素、基本方法和流

程;等级保护基本要求,了解《信息系统安全等级保护基本要求》(GB/T 22239)的主要内容,掌握5个信息系统安全保护等级对应的安全保护能力级别,掌握管理基本要求包含的5个方面以及安全技术要求包含的5个方面,等级保护其他重要标准,了解《信息系统安全等级保护实施指南》和《信息系统安全等级保护定级指南》的主要内容。

9.1 安全标准化概述

信息安全标准化工作对于解决信息安全问题具有重要的技术支撑作用。信息安全标准化不仅关系到国家安全,同时也是保护国家利益、促进产业发展的一种重要手段。在互联网飞速发展的今天,网络和信息安全问题不容忽视,积极推动信息安全标准化,牢牢掌握在信息时代全球化竞争中主动权是非常重要的。由此可以看出,信息安全标准化工作是一项艰巨、长期的基础性工作。

9.1.1 信息安全标准化概况

1. 标准和标准化的基本概念

标准是为了在一定范围内获得最佳秩序,经协商一致制定并由公认机构批准,共同使用的和重复使用的一种规范性文件。标准化是指为了在一定范围内获得最佳秩序,对现实问题或潜在问题制定共同使用和重复使用的条款的活动。

信息安全标准是确保信息安全产品和系统在设计、研发、生产、建设、使用、测评中解决其一致性、可靠性、可控性、先进性和符合性的技术规范、技术依据。我国标准化工作者根据自己的实践,用自己的语言,总结了"简化、统一、协调、优选"的八字原理,成为我国标准化界的一种共识。

2. 标准和标准化组织

早在1977年,世界上就出现了第一个数据加密标准,这是国外乃至国际上信息安全标准化工作的开端。随着通信和计算机网络的发展,国际上信息安全标准化的工作也于20世纪80年代有了较快进展,在20世纪90年代已经引起了世界各国的关注。目前世界上与信息安全标准化的组织主要有国际标准化组织(ISO)、国际电工委员会(IEC)、国际电信联盟等。

随着在世界范围内信息化水平的不断发展和贸易全球一体化的不断普及和深入,信息系统在商业和政府组织中得到了真正的广泛应用。许多组织对其信息系统不断增长的依赖性,加上在信息系统上运作业务的风险、收益和机会,使得信息安全管理成为企业管理越来越关键的一部分;在很多的场合,它已经成为一个组织生死存亡或贸易亏盈成败的起决定性的因素,因此信息安全逐渐成为人们关注的焦点。正是在这样的世界大环境和学术界共同认同的原则下,各国的研究机构都纷纷研究和制定信息安全管理、风险评估、信息安全技术的标准。国际标准就是由国际标准化组织或国际标准组织通过并公开发布的标准。而国家标准,则是由国家标准机构通过并公开发布的标准。国际标准化组织,是其成员向每个国家有关机构开放的标准化组织。在国家层面上承认的,有资格成为相应的国际和区域标准组织的国家成员的标准机构被称为国家标准机构。

3. 标准化的特点

标准化有4个特点,分别是标准化的对象(共同的、可重复的事物)、标准化的动态性、标

准化的相对性和标准化的效益。

标准化是一项活动,是制定、发布和实施标准的系统过程,标准是标准化活动过程的核心要素。标准化对象不是孤立的一件事、一个事物,而是共同的、可重复的事物,可以概括为“物”、“事”、“人”3 个方面,由于这些“物”、“事”、“人”的多次重复活动,产生了统一标准的客观需要和要求,从而分别形成了技术标准、管理标准和工作标准。

标准化是一个动态的概念,是随着科技的进步和社会的发展而不断变化发展的。标准没有最终成果,标准在深度上的持续深化和广度上的不断扩张体现了标准化的动态特征。

标准化是一个相对的概念,表现在随着事物的发展,标准化与非标准化、共性和个性的相互不断转化的发展规律上。任何已经标准化的事物和概念,都可能随着社会的发展,环境的变化,突破已有的共同规定,成为非标准化。因此,这种事物和概念的标准化—非标准化—再标准化,共性—个性—共性的交替进化,符合否定之否定的辩证法,它推动标准化永无止境地发展。

标准化的经济和社会效益只有当标准在实践中得到应用以后才能体现出来,因此在标准化活动中,标准的应用是最重要、最具实践性的一个环节,没有标准的应用,标准化工作就失去根本意义。

4. 标准化的原则

标准化的四原则分别是简化、统一、协调、优化。简化是指在一定范围内缩减对象的类型数目,使之在既定时间内足以满足一般需要的标准化形式。对象的多样性发展规模超出必要的范围时,消除多余的、可替换的、低功能的环节,保持其构成的精炼、合理,使总体功能最佳。统一是指把同类事物两种以上的表现形态归并为一种或限定在一个范围内的标准化形式。统一化的目的是消除由于不必要的多样化而造成的混乱,为人类的正常活动建立共同遵循的秩序。协调是指任何事物处于广泛联系之中,存在着相关性,其在系统中作为一个功能单元,既受约束,又影响整个功能的发挥,必须与其他功能单元进行协调,在连接点上找到一致性,使整体功能最佳。优化即按照特定的目标,在一定的限制条件下,对标准系统的构成因素及其关系进行选择、设计或调整,使之达到最理想的效果。

5. 标准的作用

(1)标准是进行贸易的基本条件。贸易双方进行货物和服务交换时,技术标准对贸易对象的形式、功能和其他技术特性所做的一致性规定,为贸易双方提供了一种共同背景、共同语言和共同的客观依据,这是对外贸易得以顺利进行的基本要求。因此,技术标准为消除贸易壁垒和建立统一市场创造了条件。在一定意义上说,没有标准就没有贸易。

(2)标准能够提高企业的经济效益。企业可以将技术标准作为打开市场的战略性手段。通过制定和执行先进的标准,抢占世界市场,并在较长时期内保持个体的持续竞争优势,实现企业利润的持续增长。世界上一些著名的跨国公司,往往都制定了较高的企业技术标准体系,以保证其竞争目标和利润的实现。

(3)标准能够提高国民经济效益。通过标准化活动,可以提高资源(自然资源、劳动、资本和技术等)的利用效率,减少资源的耗费,促进国家经济的持续发展;一些发达国家把技术标准作为提高整个国家竞争力的主要手段,通过制定技术标准,在提高本国产品竞争力的同时,削弱发展中国家产品的比较优势,促进和扩大本国技术和产品的出口,获取更大的经济效益。技术标准推广的速度、应用的范围和产生的效益要远远高于技术成果本身,其带来的

国民经济效益的增长更加明显和迅速。

6. 我国标准化领域的主要法规文件

我国标准化领域的法规文件主要有中华人民共和国标准化法、中华人民共和国标准化法实施条例、中华人民共和国标准化法条文解释、国家标准化管理办法、行业标准化管理办法、地方标准化管理办法、企业标准化管理办法、农业标准化管理办法、能源标准化管理办法、信息分类编码标准化管理办法、采用国际标准化管理办法、全国专业标准化技术委员会章程。

7. 我国国家标准的代码

(1) 强制性标准(GB)。中华人民共和国国家标准,简称国标,是包括编码系统的国家标准码,都能由在国际标准化组织(ISO)和国际电工委员会(或称国际电工协会,IEC)代表中华人民共和国的会员机构:国家标准化管理委员会发布。国标具有法律属性。一经颁布必须贯彻执行,违反则构成经济或法律方面的责任。

(2) 一般包括全国必须统一的基础标准、通用试验检验方法标准、对国计民生有重大影响的产品标准和工程建设标准、有关人身健康和生命安全和环境保护方面的标准等。

(3) 推荐性标准(GB/T)。推荐性标准是自愿采用的标准。但一经法律或法规引用,或各方商定同意纳入商品、经济合同之中,就成为共同遵守的技术依据,具有法律上的约束性,因此必须严格贯彻执行。

(4) 强制标准冠以 GB。推荐标准冠以 GB/T。与很多 ISO 国际标准相比,很多国家标准等同采用(IDT,IDentical To 其他标准)、修改采用(MOD,MODified in relation to 其他标准;2000 年以前称为“等效采用,EQV, EQuiValent to 其他标准)或非等效采用(NEQ,Not EQuivalent to 其他标准)。

(5) 国家标准化指导性技术文件(GB/Z)。国家标准化指导性技术文件,是指为适应某些领域标准快速发展和快速变化的需要,于 1998 年规定在四级标准之外,增加一种“国家标准化指导性技术文件”,作为对国家标准的补充,其代号为 GB/Z。指导性技术文件仅供使用者参考。指导性国标是指生产、交换、使用等方面,由组织(企业)自愿采用的国家标准,不具有强制性,也不具有法律上的约束性,只是相关方约定参照的技术依据。制定国家标准化指导性技术文件只在下面给定的情况下才考虑:

① 对仍处于技术发展过程中(如变化快的高新技术领域),或者由于其他理由,将来而不是现在有可能。

② 就国家标准取得一致性意见的国家标准化指导性技术文件项目。

③ 国家标准化指导性技术文件的理由及它与将来的国家标准的关系,应在前言中说明。

④ 国家标准化指导性技术文件的复审。国家标准化指导性技术文件在实施后 3 年内必须进行复审。复审结果的可能是再延长 3 年、转为国家标准或撤销。

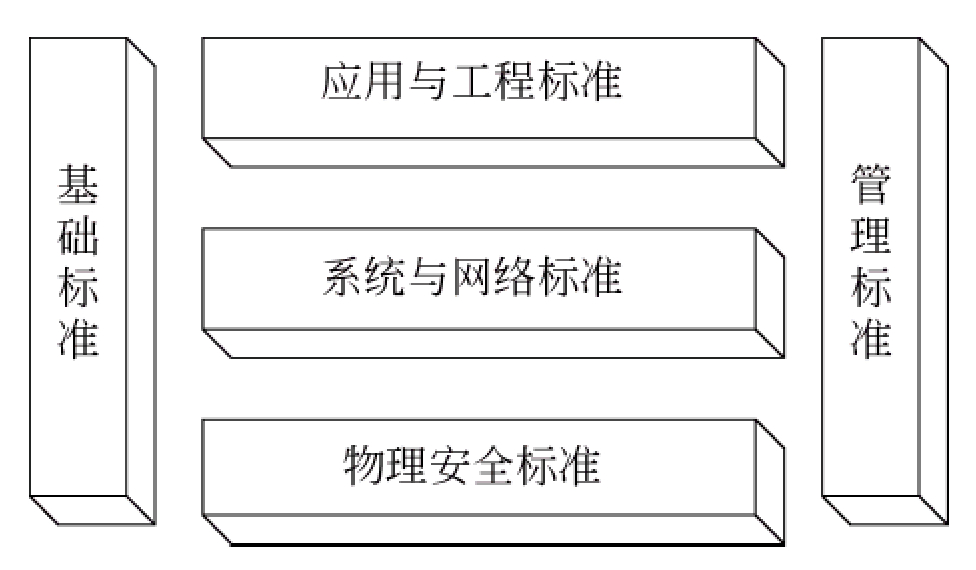


图 9.2 我国信息安全标准体系框架

8. 我国信息安全标准体系框架

我国初步形成了如图 9.2 所示的以信息安全基础标准和信息安全管理标准为支柱,以物理安全标准、系统与网络标准、应用与工程标准为

支撑的信息安全标准体系框架。

9.1.2 信息安全标准化组织

1. 国际信息安全标准化组织

目前世界上有近300个国际和区域性组织制定标准或技术规则，与信息安全标准化有关的国际组织主要有以下几个。

(1) JTC1其他分技术委员会主要包含以下几方面。

SC6——系统间通信与信息交换，主要开发开放系统互联下4层安全模型和安全协议，如ISO 9160、ISO/IEC 11557。

SC17——识别卡和有关设备，主要开发与识别卡有关的安全标准。

SC18——文件处理及有关通信，主要开发电子邮件、消息处理系统等安全标准。

SC21——开放系统互联、数据管理和开放式分布处理，主要开发开放系统互联安全体系结构、各种安全框架、高层安全模型等标准，如ISO/IEC 7498-2、ISO/IEC 9594-1～8。

SC22——程序语言，其环境及系统软件接口，也开发相应的安全标准。

SC30——开放式电子数据交换，主要开发电子数据交换的有关安全标准。如ISO 9735-9、ISO 9735-10。

(2) ISO/TC 68为银行及相关金融业务相关国际标准化组织。

(3) IEC国际电工委员会，除与ISO联合成立了JTC1外，还在电信、电子系统、信息技术和电磁兼容等方面成立技术委员会负责安全标准研制，如TC56可靠性、TC74 IT设备安全和功效、TC77电磁兼容、CISPR无线电干扰特别委员会等。

(4) ITU-T国际电信联盟，主要负责研究通信系统安全标准。它的前身是CCITT。ITU-T单独或与ISO联合开发了消息处理系统(MHS)、目录系统(X.400系列、X.500系列)和安全框架，安全模型等信息安全标准，其中的X.509标准是开展电子商务认证的重要基础标准。

(5) IETF互联网工程任务组，它主要关注与互联网有关的网络与信息安全问题，其请求注解是业界公认的事实标准。IETF一直设有专门的安全研究领域，负责研究网络授权、认证、审计与安全保护有关的协议和标准。

目前，IETF有关信息安全的工作组有BTNS、DKIM、EMU、HOKEY、ISMS、KEYPROV、KITTEN、KRB-WG、LTANS、MSEC、NEA、OPENPGP、PKIX、SASL、SMIME、SYSLOG、TLS等17个。

2. 美国标准化组织

美国国家标准学会是非营利性质的民间标准化团体，但它实际上已成为美国国家标准化中心，美国各界标准化活动都围绕它进行。

(1) ANSI美国国家标准学会，它协调并指导美国全国的标准化活动，给标准制定、研究和使用单位以帮助、提供国内外标准化情报。同时，又起着美国标准化行政管理机关的作用，如NCITS-T4制定IT安全技术标准、X9制定金融业务标准、X12制定商业交易标准(EDI)等。

(2) NIST美国国家标准与技术研究院(直属美国商务部，从事物理、生物和工程方面的基础和应用研究，以及测量技术和测试方法方面的研究，提供标准、标准参考数据及有关服

务，在国际上享有很高的声誉。此外，NIST 负责联邦政府非密敏感信息。

(3) DOD 美国国防部标准化文件，他负责涉密信息、NSA 以及国防部指令(DODDI)(如 TCSEC)。

(4) IEEE 美国电气和电子工程师协会，是美国规模最大的专业协会。在电气及电子工程、计算机及控制技术领域中，IEEE 发表的文献占了全球近 30%。

3. 我国标准化组织

1984 年，成立数据加密技术分委员会，后来改为信息技术安全分技术委员会。

2002 年 4 月，为加强信息安全标准的协调工作，国家标准委员会决定成立信息安全标准委员会，由国家标准委员会直接领导，对口 ISO/IEC JTC1 SC27；秘书处设在中国电子技术标准化研究所；委员会由 30 多个部门和单位的 49 名领导和专家组成，目前共有工作组成员单位 165 家，其中企业 120 家。

国家标准委员会高新函[2004]1 号文决定，自 2004 年 1 月起，各有关部门在申报信息安全国家标准计划项目时，必须经信息安全标准委员会提出工作意见，协调一致后由信息安全标准委员会组织申报；在国家标准制定过程中，标准工作组或主要起草单位要与信息安全标准委员会积极合作，并由信息安全标准委员会完成国家标准送审、报批工作。

4. 全国信息安全标准化技术委员会 TC260 的组织结构图

全国信息安全标准化技术委员会的成立标志着我国信息安全标准化工作，步入了“统一领导、协调发展”的新时期。该标准委员会是在信息安全的专业领域内，从事信息安全标准化工作的技术工作组织。它的工作任务是向国家标准化管理委员会提出本专业标准化工作的方针、政策和技术措施的建议。信息安全标准委员会将协调各有关部门，本着平等、公开、协商的原则组织提出一套系统、全面、分布合理的信息安全标准体系，以信息安全标准体系为工作依据有步骤、有计划地进行信息安全标准的制定工作。信息安全标准委员会主要以工作组形式开展工作，如图 9.3 所示。为进一步推进信息安全标准委员会的工作，尽快启动一批信息安全关键性标准的研究工作，经信息安全标准委员会秘书处研究，并通报信息安全标准委员会主任委员及副主任委员同意，启动信息安全标准体系与协调工作组的工作。

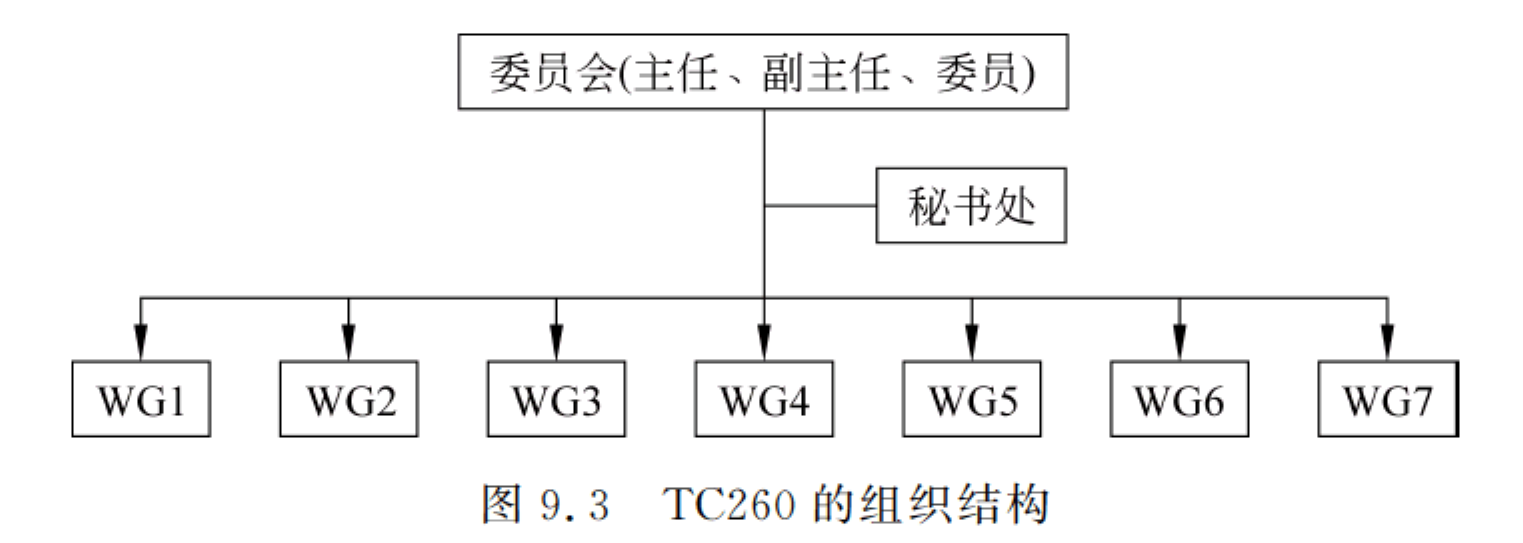


图 9.3　TC260 的组织结构

全国信息安全标准化技术委员会各组织的工作如下：

秘书处负责委员会的日常事务工作。秘书处是委员会的常设办事机构，负责委员会的日常事务工作。秘书处设在中国电子技术标准化研究所。

信息安全标准体系与协调工作组(WG1)负责研究信息安全标准体系，跟踪国际标准发展动态，研究信息安全标准需求，研究并提出新工作项目及设立新工作组的建议，并协调各工作组项目。

涉密信息系统安全保密标准工作组(WG2)研究提出涉密信息系统安全保密标准体系。

制定和修订涉密信息系统安全保密标准。

密码技术标准工作组（WG3）研究提出商用密码技术标准体系。研究制定商用密码算法、商用密码模块和商用密钥管理等相关标准。

鉴别与授权工作组（WG4）研究制定鉴别与授权标准体系，包括调研国内相关标准需求、研究制定鉴别与授权标准。

信息安全评估工作组（WG5）调研测评标准现状与发展趋势，研究我国统一测评标准体系的思路和框架，提出测评标准体系。研究制订急需的测评标准。

通信安全标准工作组（WG6）调研通信安全标准现状与发展趋势，研究提出通信安全标准体系，研究制订急需的通信安全标准。

信息安全管理工作组（WG7）研究信息安全管理动态，调研国内管理标准需求，研究提出信息安全管理标准体系，制定信息安全管理相关标准。

9.2 信息安全评估标准

目前世界上有很多国际和区域性组织制定标准或技术规则与信息安全标准化有关的组织。主要有国际标准化组织（ISO）、国际电工委员会（IEC）、国际电信联盟（RITU）、工程任务组（IETF）等。我国信息安全标准化工作自从加入 WTO 后，已制定了一批符合中国国情的信息安全标准，一些重点行业还颁布了一批信息安全的行业标准，为我国信息安全技术的发展做出了很大的贡献。

现有的信息安全评估标准主要采用定性分析法对风险进行分析，即通常采取安全事件发生的概率来计算风险。然而，在安全评估过程中，评估人员常常面临的问题是信息资产的重要性，如何度量资产，如何分级，什么样的系统损失可能构成什么样的经济损失，如何构建技术体系和管理体系达到预定的安全等级，如何计算如果黑客入侵，尽管没有造成较大的经济损失，但企业的名誉损失又该如何衡量。另外，对企业的管理人员而言，哪些风险在企业可承受的范围内。这些问题从不同角度决定了一个信息系统安全评估的结果。目前的信息安全评估标准都不能对这些问题进行分析。当前一些研究人员正在探讨的“网络控制论”、“自动化分析工具”和“形式化分析方法”等新理论、新方法有可能为未来的风险评估和管理提供一些新的、可借鉴的方法和工具。在没有一个统一的信息安全评估标准的情况下，各家专业评估公司大多数是凭借各自积累的经验解决。因此，这就需要统一的信息安全评估标准的出台。目前，信息安全风险管理中存在的诸多问题也只能在实践中、发展中加以解决。

1. 美国的安全评测标准（TCSEC）

TCSEC 标准是计算机系统安全评估的第一个正式标准，具有划时代的意义。该准则于 1970 年由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。TCSEC 最初只是军用标准，后来延至民用领域。TCSEC 将计算机系统的安全划分为 4 个等级、7 个级别。全称美国可信计算机安全评价标准（TCSEC）。

美国安全测评标准是于 1970 年由美国国防科学委员会提出，1985 年公布，主要为军用标准，后来延至民用领域。其安全级别从高到低分为 A、B、C、D 四级，级下再分小类，即 A1、B3、B2、B1、C2、C1、D。它的分级分类主要依据 4 个准则——安全政策、可控性、保证能力、文档。

2. 欧洲的安全评测标准(ITSEC)

欧洲安全测评标准是欧洲多国安全评价方法的综合产物,作用范围是军用、政府用和商用。它以超越 TCSEC 为目的,将安全概念分为功能与功能评估两部分。功能准则在测定上分 F1～F10 共 10 级,1～5 级对应于 TCSEC 的 D～A,6～10 级加上了以下概念:

F6:数据和程序的完整性。

F7:系统可用性。

F8:数据通信完整性。

F9:数据通信保密性。

F10:包括机密性和完整性的网络安全。

评估准则分为 6 级:

E1:测试。

E2:配置控制和可控的分配。

E3:能访问详细设计和源代码。

E4:详细的脆弱性分析。

E5:设计与源代码明显对应。

E6:设计与源代码在形式上一致。

3. 加拿大的评测标准(CTCPEC)

加拿大测评标准(Canadian Trusted Computer Product Evaluation Criteria,CTCPEC)于 1989 年公布,专为政府需求而设计。它与 ITSEC 类似,将安全分为功能性需求和保证性需求两部分。它的功能性要求分为四大类,即机密性、完整性、可用性、可控性。在每种安全需求下又分成很多小类,表示安全性上的差别,分级条数为 0～5 级。

4. 美国联邦准则(FC)

美国联邦准则是对 TCSEC 的升级,于 1992 年 12 月公布,它引入了"保护轮廓(PP)"这一重要概念,每个轮廓都包括功能部分、开发保证部分和评测部分。它的分级方式与 TCSEC 不同,它吸取了 ITSEC、CTCPEC 的优点,并且供美国政府用、民用和商用。

5. 通用准则(CC)

通用准则是国际标准化组织统一现有多种准则的努力结果;它于 1993 年开始实行,于 1996 年推出 V1.0 版本,1998 年推出 V2.0 版本,1999 年 6 月正式成为国际标准,并且在 1999 年 12 月 ISO 出版发行 ISO/IEC 15408;通用准则的主要思想和框架取自 ITSEC 和 FC;它充分突出了"保护轮廓",将评估过程分为"功能"和"保证"两部分,是目前最全面的评价准则,也是国际上认同的表达 IT 安全的体系结构。通用准则是一组规则集,也是一种评估方法,其评估结果国际互认。通用测试方法(CEM)是已有安全准则的总结和兼容。它采用通用的表达方式,便于理解。此外,通用准则有灵活的架构,可以定义自己的要求扩展 CC 要求。

6. GB/T 18336(ISO 15408)

简介和一般模型,是 GB/T 18336 的介绍。它定义了 IT 安全性评估的一般概念和原理,并提出了评估的一般模型。第一部分也提出了若干结构,这些结构可用于表达 IT 安全目的,用于选择和定义 IT 安全要求,以及用于书写产品和系统的高层规范。另外,针对各种目标选择,描述标准的每一部分的有效性。

安全功能要求规定了一系列功能组件,作为表达 TOE 功能要求的标准方法。第二部分列出了一系列功能组件、族和类。

安全保证要求规定了一系列保证组件,作为表达 TOE 保证要求的标准方法。第三部分列出了一系列保证组件、族和类。第三部分也定义了 PP 和 ST 的评估准则,并提出了一些评估保证级别,这些级别定义了划分 TOE 保证等级的预定义的 GB/T 18336 尺度,通常称为评估保证级(EAL)。

7. GB/T 18336(CC)的目标读者

GB/T 18336(CC)的目标读者包括 TOE(评估对象)的客户、开发者和评估者,此外,还包括系统管理员和系统安全管理员、内部和外部审计员、安全架构师和设计师、认可者、评估发起者与评估管理机构等。

9.3 信息安全管理标准

9.3.1 国际信息安全管理重要标准

ISO/IEC 27001:2005 的名称是 Information technology-Security techniques-Information security management systems-requirements(信息技术-安全技术-信息安全管理体系-要求),它是解释建立和维护文档化的 ISMS 的要求,也是依照 ISO 27001 对组织的 ISMS 进行审核认证的基础。ISO 27001 标准对信息安全管理体系(ISMS)并没有一个十分明确的定义,可以将其理解为组织管理体系的一部分。ISMS 涉及的内容:用于组织信息资产风险管理、确保组织信息安全的、包括为制定、实施、评审和维护信息安全策略所需的组织机构、目标、职责、程序、过程和资源。标准要求的 ISMS 建立过程:制定信息安全方针策略,明确体系范围,明确管理职责,通过风险评估确定控制目标和控制方式。遵循 PDCA。体系一旦建立,组织应该按规定要求进行运作,保持体系的有效性。ISMS 应形成一定的文档,包括方针策略、适用性声明文件和实施安全控制所需的程序文件。一个文档化的 ISMS 应该阐述要保护的资产、组织进行风险管理的途径、控制目标和控制方式、需要的保障程度。

ISO/IEC 27002:2007 的名称是 Information technology-Security techniques-Code of practice for information security management(信息技术-安全技术-信息安全管理实用规则),本标准给出了一个组织启动、实施、保持和改进信息安全管理的指南和一般原则。另外,本标准列出的目标为通常所接受的信息安全管理的目的提供了指导。而且,本标准的控制目标和控制措施的实施旨在满足风险评估所识别的要求。最后,本标准可作为建立组织的安全准则和有效安全管理惯例的实用指南,并有利于在组织间的活动中建立信心。

9.3.2 我国信息安全管理重要标准

《信息安全风险评估规范》(GB/T 20984)提出了风险评估的基本概念、要素关系、分析原理、实施流程和评估方法,以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。本标准适用于规范组织开展的风险评估工作。

《信息安全风险管理规范》(GB/Z 24364)针对信息安全风险管理所涉及的对象确立、风险评估、风险处理、审核批准、沟通咨询等不同过程进行了综合性描述和规范,对信息安全风

险管理在信息系统生命周期各阶段的应用作了系统阐述，并经过国家有关行业和地区的试点验证。

《信息安全事件管理指南》(GB/Z 20985)规范了信息安全事件的管理，概括性地介绍了信息安全事件管理、采用信息安全事件管理方案的益处以及与采用方案相关的关键问题，明确阐述了规划和制定信息安全事件管理策略和方案的相关步骤，详细说明了管理信息安全事件和开展事件善后工作的过程和规程。本指导性技术文件可用于指导信息安全管理者，信息系统、服务和网络管理者对信息安全事件的管理。

《信息安全事件分类分级指南》(GB/Z 20986)为信息安全事件的分类分级提供指导，用于信息安全事件的防范与处置，为事前准备、事中应对、事后处理提供一个基础指南，可供信息系统和基础信息传输网络的运营和使用单位以及信息安全主管部门参考使用。信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等 7 个基本分类，每个基本分类分别包括若干个子类。

《信息系统灾难恢复规范》(GB/T 20988)规定了信息系统灾难恢复应遵循的基本要求。本标准适用于信息系统灾难恢复的规划、审批、实施和管理。信息系统的灾难恢复工作，包括灾难恢复规划和灾难备份中心的日常运行、关键业务功能在灾难备份中心的恢复和继续运行，以及主系统的灾后重建和回退工作，还涉及突发事件发生后的应急响应。

9.4 等级保护标准

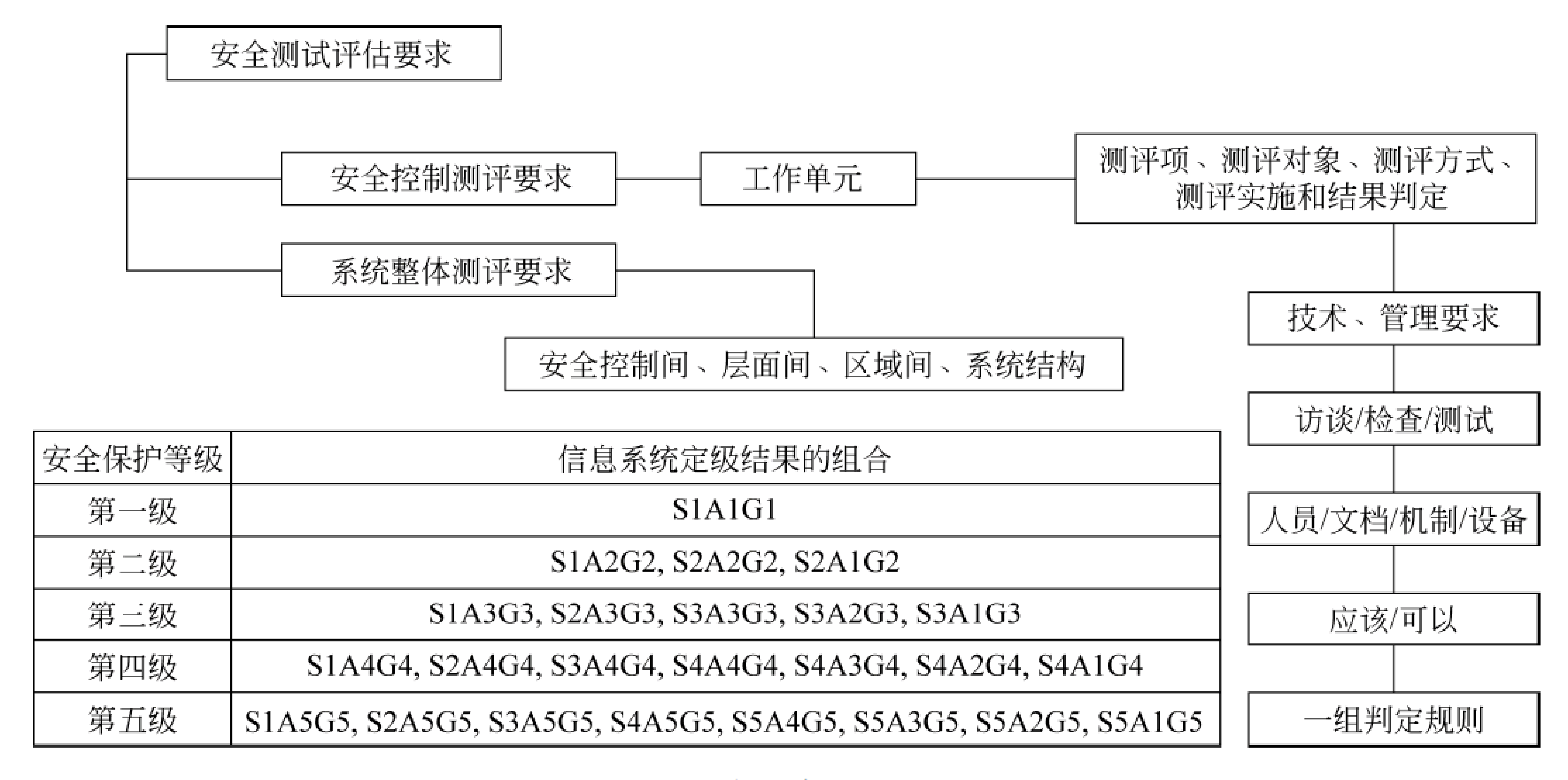
《中华人民共和国计算机信息系统安全保护条例》(1994 年国务院 147 号令)第 9 条：计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。

信息安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，在中国、美国等很多国家都存在的一种信息安全领域的工作。在中国，信息安全等级保护广义上为涉及该工作的标准、产品、系统、信息等均依据等级保护思想的安全工作；狭义上称为的一般指信息系统安全等级保护，是指对国家安全、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置的综合性工作。

9.4.1 信息安全等级保护基本要求

《信息安全等级保护基本要求》是信息安全等级保护相关系列标准之一。与该标准相关的系列标准包括《信息安全技术信息系统安全等级保护定级指南》(GB/T 22240—2008)、《信息安全技术信息系统安全等级保护基本要求》(GB/T 22239—2008)、《信息安全技术信息系统安全等级保护实施指南》(GB/T AAAA—AAAA)。一般来说，信息系统需要靠多种安全措施进行综合防范以降低其面临的安全风险。该标准针对信息系统中的单项安全措施和多个安全措施的综合防范，对应地提出单元测评和整体测评的技术要求，用以指导测评人员从信息安全等级保护的角度对信息系统进行测试评估。单元测评对安全技术和安全管理

上各个层面的安全控制点提出不同安全保护等级的测评要求。整体测评根据安全控制点间、层面间和区域间相互关联关系以及信息系统整体结构对信息系统整体安全保护能力的影响提出测评要求。该标准给出了等级测评结论中应包括的主要内容,未规定给出测评结论的具体方法和量化指标。内容如图 9.4 所示。



安全保护等级	信息系统定级结果的组合
第一级	S1A1G1
第二级	S1A2G2, S2A2G2, S2A1G2
第三级	S1A3G3, S2A3G3, S3A3G3, S3A2G3, S3A1G3
第四级	S1A4G4, S2A4G4, S3A4G4, S4A4G4, S4A3G4, S4A2G4, S4A1G4
第五级	S1A5G5, S2A5G5, S3A5G5, S4A5G5, S5A4G5, S5A3G5, S5A2G5, S5A1G5

图 9.4　基本要求 GB/T 22239

该标准的使用方法:该标准中针对每一个安全控制点的测评就构成一个单元测评,单元测评中的每一个具体测评实施要求项是与安全控制点下面所包括的要求项(测评指标)相对应的。在对每一要求项进行测评时,可能用到访谈、检查和测试 3 种测试方法,也可能用到其中一种或两种,为了描述简洁,在测评要求项中,没有针对每一个要求项分别进行描述,而是对具有相同测评方法的多个要求项进行了合并描述,使用时,应当从单元测评的测评实施中抽取出对于《信息安全技术信息系统安全等级保护基本要求》(GB/T 22239—2008)中每一个要求项的测评要求,并按照这些测评要求开发测评指导书,以规范和指导安全等级测评活动。测评过程中,测评人员应注意对测评记录和证据的采集、处理、存储和销毁,保护其在测评期间免遭破坏、更改或遗失,并保守秘密。测评的最终输出是测评报告。

1. 信息系统安全等级保护测评要求

(1) 测评的范围。该标准规定了对信息系统安全等级保护状况进行安全测试评估的要求,包括对第一级信息系统、第二级信息系统、第三级信息系统和第四级信息系统进行安全测试评估的单元测评要求和信息系统整体测评要求。该标准略去对第五级信息系统进行单元测评的具体内容要求。该标准适用于信息安全测评服务机构、信息系统的主管部门及运营使用单位对信息系统安全等级保护状况进行的安全测试评估。信息安全监管职能部门依法进行的信息安全等级保护监督检查可以参考使用。

(2) 等级保护需要遵循的原则。

① 客观性和公正性原则。测评工作虽然不能完全摆脱个人主张或判断,但测评人员应当在没有偏见和最小主观判断情形下,按照测评双方相互认可的测评方案,基于明确定义的测评方法和过程,实施测评活动。

② 经济性和可重用性原则。基于测评成本和工作复杂性考虑，鼓励测评工作重用以前的测评结果，包括商业安全产品测评结果和信息系统先前的安全测评结果。所有重用的结果，都应基于这些结果还能适用于目前的系统，能反映目前系统的安全状态。

③ 可重复性和可再现性原则。无论谁执行测评，依照同样的要求，使用同样的方法，对每个测评实施过程的重复执行都应该得到同样的测评结果。可再现性体现在不同测评者执行相同测评结果的一致性。可重复性体现在同一测评者重复执行相同测评结果的一致性。

④ 符合性原则。测评所产生的结果应当是在对测评指标的正确理解下所取得的良好的判断。测评实施过程应当使用正确的方法以确保其满足了测评指标的要求。

(3) 测评内容。信息系统安全等级测评主要包括单元测评和整体测评两部分。单元测评是等级测评工作的基本活动，每个单元测评包括测评指标、测评实施和结果判定三部分。其中，测评指标来源于《信息安全技术信息系统安全等级保护基本要求》(GB/T 22239—2008)中的第五级目录中的各要求项。测评实施描述测评过程中使用的具体测评方法、涉及的测评对象和具体测评取证过程的要求等。整体测评是在单元测评的基础上，通过进一步分析信息系统的整体安全性，对信息系统实施的综合安全测评。整体测评主要包括安全控制点间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等。整体测评需要与信息系统的实际情况相结合，因此全面地给出整体测评要求的全部内容、具体实施过程和明确的结果判定方法是非常困难的，测评人员应根据被测系统的实际情况，结合本标准的要求，实施整体测评。

(4) 测评方法。它指测评人员在测评实施过程中所使用的方法，主要包括访谈、检查和测试 3 种测评方法。其中，访谈是指测评人员通过引导信息系统相关人员进行有目的的(有针对性的)交流以帮助测评人员理解、分析或取得证据的过程，检查是指测评人员通过对测评对象(如管理制度、操作记录、安全配置等)进行观察、查验、分析以帮助测评人员理解、分析或取得证据的过程，测试是测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看和分析结果以帮助测评人员获取证据的过程。

测评对象指测评实施的对象，即测评过程中涉及的信息系统的相关人员、制度文档、各类设备及其安全配置等。

(5) 测评力度。它是在测评过程中实施测评工作的力度，反映测评的广度和深度，体现为测评工作的实际投入程度。测评广度越大，测评实施的范围越大，测评实施包含的测评对象就越多；测评深度越深，越需要在细节上展开，测评就越严格，因此就越需要更多的投入。投入越多，测评力度就越强，测评就越有保证。测评的广度和深度落实到访谈、检查和测试 3 种不同的测评方法上，能体现出测评实施过程中访谈、检查和测试的投入程度的不同，如表 9.1 所示。

信息安全等级保护要求不同安全保护等级的信息系统应具有不同的安全保护能力，满足相应等级的保护要求。为了检验不同安全保护等级的信息系统是否具有相应等级的安全保护能力，是否满足相应等级的保护要求，需要实施与其安全保护等级相适应的测评，付出相应的工作投入，达到应有的测评力度。第一级到第四级信息系统的测评力度反映在访谈、检查和测试等 3 种基本测评方法的测评广度和深度上，落实在不同单元测评中具体的测评实施上。

表 9.1　测试力度

测评力度		信息安全等级			
		第一级	第二级	第三级	第四级
访谈	广度	种类和数量上抽样，较少	种类和数量上抽样，均较多	数量上抽样，基本上覆盖	数量上抽样，基本上覆盖
	深度	简要	充分	较全面	较全面
检查	广度	种类和数量上抽样，较少	种类和数量上抽样，均较多	数量上抽样，基本上覆盖	数量上抽样，基本上覆盖
	深度	简要	充分	较全面	全面
测试	广度	种类、数量和范围上抽样，种类数量较少，范围小	种类、数量和范围上抽样，种类数量较多，范围较大	数量、范围上抽样，基本上覆盖	数量、范围上抽样，基本上覆盖
	深度	功能测试、性能测试	功能测试、性能测试	功能测试、性能测试、渗透测试	功能测试、性能测试、渗透测试

(6) 结果重用。在信息系统中，有些安全控制可以不依赖于其所在的地点便可测评，即在其部署到运行环境之前便可以接受安全测评。一些商用安全产品的测评就属于这种安全测评。如果一个信息系统部署和安装在多个地点，且系统具有一组共同的软件、硬件、固件等组成部分，对这些安全控制的测评可以集中在一个集成测试环境中实施，如果没有这种环境，则可以在其中一个预定的运行地点实施，在其他运行地点的安全测评便可重用此测评结果。

在信息系统所有安全控制中，有一些安全控制与它所处的运行环境紧密相关(如与人员或物理有关的某些安全控制)，对其测评必须在分发到相应运行环境中才能进行。如果多个信息系统处在地域邻近的封闭场地内，系统所属的机构在同一个领导层管理之下，对这些安全控制在多个信息系统中进行重复测评，可能是对有效资源的一种浪费。因此，可以在一个选定的信息系统中进行测评，其他相关信息系统可以直接重用这些测评结果。

2. 信息系统安全保护等级

信息系统根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高划分为 5 个级别。

第一级：用户自主保护级。完全由用户自己来决定如何对资源进行保护，以及采用何种方式进行保护。

第二级：系统审计保护级。本级的安全保护机制受到信息系统等级保护的指导，支持用户具有更强的自主保护能力，特别是具有访问审计能力。即能创建、维护受保护对象的访问审计跟踪记录，记录与系统安全相关事件发生的日期、时间、用户和事件类型等信息，所有和安全相关的操作都能够被记录下来，以便当系统发生安全问题时，可以根据审计记录，分析追查事故责任人，使所有的用户对自己行为的合法性负责。

第三级：安全标记保护级。除具有第二级系统审计保护级的所有功能外，它还要求对访问者和访问对象实施强制访问控制，并能够进行记录，以便事后的监督、审计。通过对访问者和访问对象指定不同安全标记，监督、限制访问者的权限，实现对访问对象的强制访问控制。

第四级：结构化保护级。将前三级的安全保护能力扩展到所有访问者和访问对象，支

持形式化的安全保护策略。其本身构造也是结构化的，将安全保护机制划分为关键部分和非关键部分，对关键部分强制性地直接控制访问者对访问对象的存取，使之具有相当强的抗渗透能力。本级的安全保护机制能够使信息系统实施一种系统化的安全保护。

第五级：访问验证保护级。这个级别除了具备前四级的所有功能外，还特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动，仲裁访问者能否访问某些对象从而对访问对象实行专控，保护信息不能被非授权获取。因此，本级的安全保护机制不易被攻击、被篡改，具有极强的抗渗透的保护能力。

3. 基本技术要求和基本管理要求

信息系统安全等级保护应依据信息系统的安全保护等级情况，保证它们具有相应等级的基本安全保护能力，不同安全保护等级的信息系统要求具有不同的安全保护能力。

基本安全要求是针对不同安全保护等级信息系统应该具有的基本安全保护能力提出的安全要求，根据实现方式的不同，基本安全要求分为基本技术要求和基本管理要求两大类。技术类安全要求与信息系统提供的技术安全机制有关，主要通过在信息系统中部署软硬件并正确地配置其安全功能来实现；管理类安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程及记录等方面做出规定来实现。

基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出；基本管理要求从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出，基本技术要求和基本管理要求是确保信息系统安全不可分割的两个部分。

基本安全要求从各个层面或方面提出了系统的每个组件应该满足的安全要求，信息系统具有的整体安全保护能力通过不同组件实现基本安全要求来保证。除了保证系统的每个组件满足基本安全要求外，还要考虑组件之间的相互关系，来保证信息系统的整体安全保护能力。

对于涉及国家秘密的信息系统，应按照国家保密工作部门的相关规定和标准进行保护。对于涉及密码的使用和管理，应按照国家密码管理的相关规定和标准实施。

4. 基本技术要求的 3 种类型

根据保护侧重点的不同，技术类安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄露、破坏和免受未授权的修改的信息安全类要求（简记为 S）；保护系统连续正常地运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为 A）；通用安全保护类要求（简记为 G）。

9.4.2 等级保护的实施指南

等级保护实施指南（GB/T 25058—2010）详细说明了等级保护实施过程中的基本原则、角色、职责、实施的基本流程和主要过程及其活动，如图 9.5 所示。

1. 信息系统安全等级保护实施过程中应遵循的基本原则

（1）自主保护原则。信息系统运营、使用单位及其主管部门按照国家相关法规和标准，自主确定信息系统的安全保护等级，自行组织实施安全保护。

（2）重点保护原则。根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。

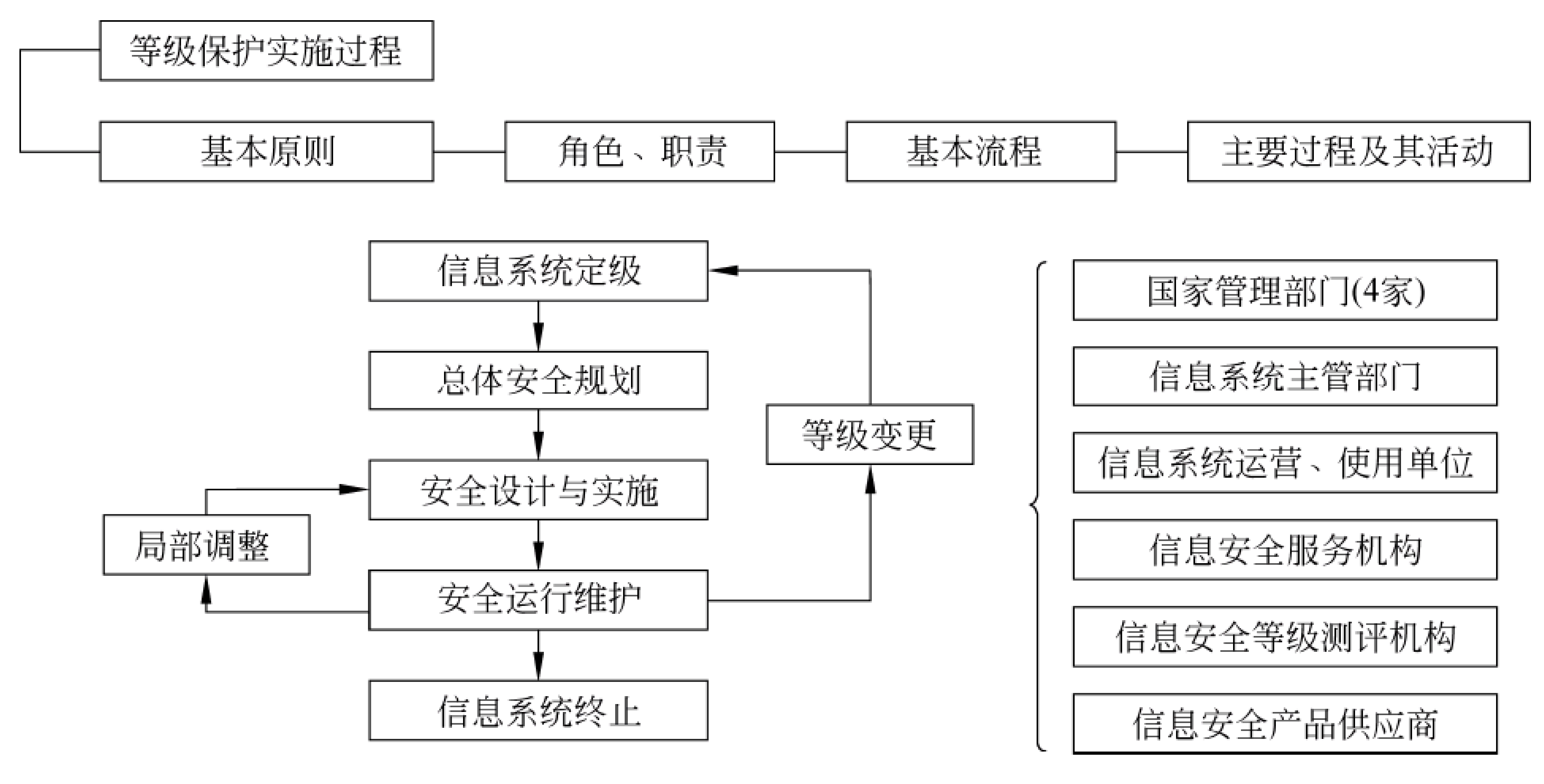


图 9.5　实施指南——GB/T 25058—2010

(3) 同步建设原则。信息系统在新建、改建、扩建时应当同步规划和设计安全方案，投入一定比例的资金建设信息安全设施，保障信息安全与信息化建设相适应。

(4) 动态调整原则。要跟踪信息系统的变化情况，调整安全保护措施。由于信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级，根据信息系统安全保护等级的调整情况，重新实施安全保护。

2. 涉及的各类角色和职责

(1) 国家管理部门。公安机关负责信息安全等级保护工作的监督、检查、指导；国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导；国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导；涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理；国务院信息化工作办公室及地方信息化领导小组办事机构负责等级保护工作的部门间协调。

(2) 信息系统主管部门。负责依照国家信息安全等级保护的管理规范和技术标准，督促、检查和指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

(3) 信息系统运营、使用单位。负责依照国家信息安全等级保护的管理规范和技术标准，确定其信息系统的安全保护等级，有主管部门的，应当报其主管部门审核批准；根据已经确定的安全保护等级，到公安机关办理备案手续；按照国家信息安全等级保护管理规范和技术标准，进行信息系统安全保护的规划设计；使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品和信息安全产品，开展信息系统安全建设或者改建工作；制定、落实各项安全管理制度，定期对信息系统的安全状况、安全保护制度及措施的落实情况进行自查，选择符合国家相关规定的等级测评机构，定期进行等级测评；制定不同等级信息安全事件的响应、处置预案，对信息系统的信息安全事件分等级进行应急处置。

(4) 信息安全服务机构。负责根据信息系统运营、使用单位的委托，依照国家信息安全等级保护的管理规范和技术标准，协助信息系统运营、使用单位完成等级保护的相关工作，包括确定其信息系统的安全保护等级、进行安全需求分析、安全总体规划、实施安全建设和

安全改造等。

(5)信息安全等级测评机构。负责根据信息系统运营、使用单位的委托或根据国家管理部门的授权,协助信息系统运营、使用单位或国家管理部门,按照国家信息安全等级保护的管理规范和技术标准,对已经完成等级保护建设的信息系统进行等级测评;对信息安全产品供应商提供的信息安全产品进行安全测评。

(6)信息安全产品供应商。负责按照国家信息安全等级保护的管理规范和技术标准,开发符合等级保护相关要求的信息安全产品,接受安全测评;按照等级保护相关要求销售信息安全产品并提供相关服务。

3. 信息系统安全等级保护实施的基本流程

在安全运行与维护阶段,信息系统因需求变化等原因导致局部调整,而系统的安全保护等级并未改变,应从安全运行与维护阶段进入安全设计与实施阶段,重新设计、调整和实施安全措施,确保满足等级保护的要求。但信息系统发生重大变更导致系统安全保护等级变化时,应从安全运行与维护阶段进入信息系统定级阶段,重新开始一轮信息安全等级保护的实施过程。

4. 等级保护主要过程

其包括信息系统定级、总体安全规划、安全设计与实施、安全运行与维护及信息系统终止。在每个过程中都详细给出了活动目标、参与角色、活动输入、活动描述等。

9.4.3 等级保护的定级指南

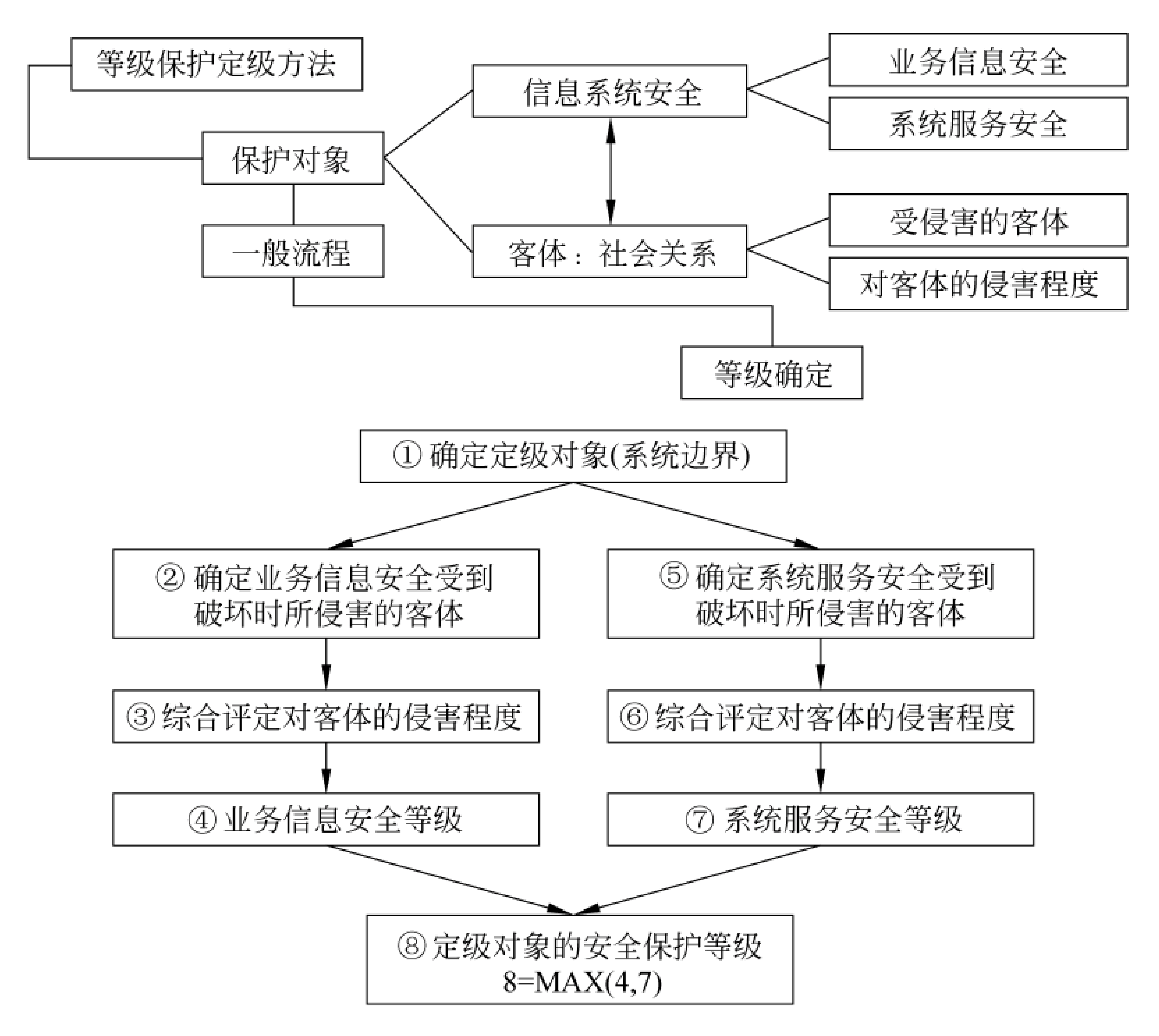
GB/T 22240 标准规定了信息系统安全等级保护的定级方法,适用于为信息系统安全等级保护的定级工作提供指导,如图 9.6 所示,该标准以信息安全等级保护工作直接作用的具体信息和信息系统为保护对象,且根据等级保护相关文件,信息系统的安全保护等级分为 5 级。

定级是等级保护工作的首要环节,是开展信息系统建设、整改、测评、备案、监督检查等后续工作的重要基础。信息系统安全级别定不准,系统建设、整改、备案、等级测评等后续工作都失去了针对性。需要特别说明的是,信息系统的安全保护等级是信息系统的客观属性,不以已采取或将采取什么安全保护措施为依据,也不以风险评估为依据,而是以信息系统的重要性和信息系统遭到破坏后对国家安全、社会稳定、人民群众合法权益的危害程度为依据,确定信息系统的安全等级。即从国家、人民群众的根本利益出发,考虑了信息系统受到损害后的最大风险。因此,各部门、各单位要高度重视定级工作,切实加强对定级工作的组织领导,科学、准确地确定信息系统等级。信息系统运营使用单位在定级时,公安网监部门可以对信息系统运营使用单位在定级工作中给予指导和帮助,保障信息系统运营使用单位科学、合理地确定定级对象和准确定级。定级工作可以参照以下几个步骤进行。

1. 摸底调查,掌握信息系统底数

按照《定级工作通知》确定的定级范围,各部委和各省(区、市)可以组织开展对所属信息系统进行摸底调查,摸清信息系统底数;掌握信息系统(包括信息网络)的业务类型、应用或服务范围、系统结构等基本情况。各部委和各省(区、市)要加强对等级保护工作的组织领导,明确责任部门,可以成立信息安全等级保护工作领导小组(以下简称领导小组),并下设等级保护工作办公室、信息系统运营使用单位成立等级保护工作组。

相关部门工作职责:领导小组办公室组织信息系统运营使用单位开展摸底调查工作,



保护对象受到破坏时受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

图 9.6　定级指南——GB/T 22240

汇总信息系统摸底调查情况，报领导小组。等级保护工作组对本单位的信息系统开展摸底调查，并上报领导小组办公室。

2. 确定定级对象

在信息系统安全等级保护定级工作（以下简称“定级工作”）中，如何科学、合理地确定定级对象是最关键、最复杂的问题。信息系统运营使用单位或主管部门按以下原则确定定级对象：一是应用系统应按照不同业务类别单独确定为定级对象，不以系统是否进行数据交换、是否独享设备为确定定级对象条件，起传输作用的基础网络要作为单独的定级对象；二是确认负责定级的单位是否对所定级系统具有安全管理责任；三是具有信息系统的基本要素。作为定级对象的信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的有形实体。应避免将某个单一的系统组件（如服务器、终端、网络设备等）作为定级对象。

例如，奥运网络主要包括“奥组委办公外网”（承载自动化办公、场馆管理、电子邮件、物流、员工之家等 16 项业务）、“奥组委内部办公局域网”（承载着财务管理、人事管理等 3 项业务）、“奥运票务网”（票务网站和票务管理系统）、“奥运官方网站”（门户网站和后台数据处理系统）、“奥运互联网接入”等 5 个奥运网络和信息系统。确定奥组委办公外网、奥组委内部

办公局域网、票务网站、票务管理系统和奥运官方网站为定级对象。

相关部门工作职责：等级保护工作组按照确定定级对象的原则确定本部门的定级对象，并上报领导小组办公室。专家组可以在确定定级对象过程中提供咨询指导。公安机关指导等级保护工作组确定定级对象。

3. 初步确定信息系统等级

信息系统的安全保护等级是信息系统的客观属性，不以已采取或将采取什么安全保护措施为依据，而是以信息系统的重要性和信息系统遭到破坏后对国家安全、社会稳定、人民群众合法权益的危害程度为依据，确定信息系统的安全保护等级。既要防止个别单位片面追求绝对安全而定级过高，也要防止为了逃避监管定级偏低。信息网络的安全等级可以参照在其上运行的信息系统的等级、网络的服务范围和自身的安全需求确定适当的保护等级，不以在其上运行的信息系统的最高等级或最低等级为标准，即不就高、不就低。

跨省或者全国统一联网运行的信息系统，可以由主管部门统一确定安全保护等级。由各行业统一规划、统一建设、统一安全保护策略的信息系统，应由各部委统一确定一个级别；由各部委统一规划、分级建设、运行的信息系统，应由部、省、地市分别确定系统等级，但各行业应对该类系统提出定级意见，避免出现同类系统定级出现较大偏差问题。

（1）定级的一般流程。信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级也应由业务信息安全和系统服务安全两方面确定。从业务信息安全角度反映的信息系统安全保护等级称业务信息安全等级。从系统服务安全角度反映的信息系统安全保护等级称系统服务安全等级。确定信息系统安全保护等级的一般流程如图 9.7 所示。确定作为定级对象的信息系统；确定业务信息安全受到破坏时所侵害的客体；根据不同的受侵害客体，从多个方面综合评定业务信息安全被破坏对客体的侵害程度；依据等级保护定级方法，得到业务信息安全等级；确定系统服务安全受到破坏时所侵害的客体；根据不同的受侵害客体，从多个方面综合评定系统服务安全被破坏对客体的侵害程度；依据对客体的损害程度，得到系统服务安全等级；由业务信息安全等级和系统服务安全等级的较高者确定定级对象的安全保护等级。

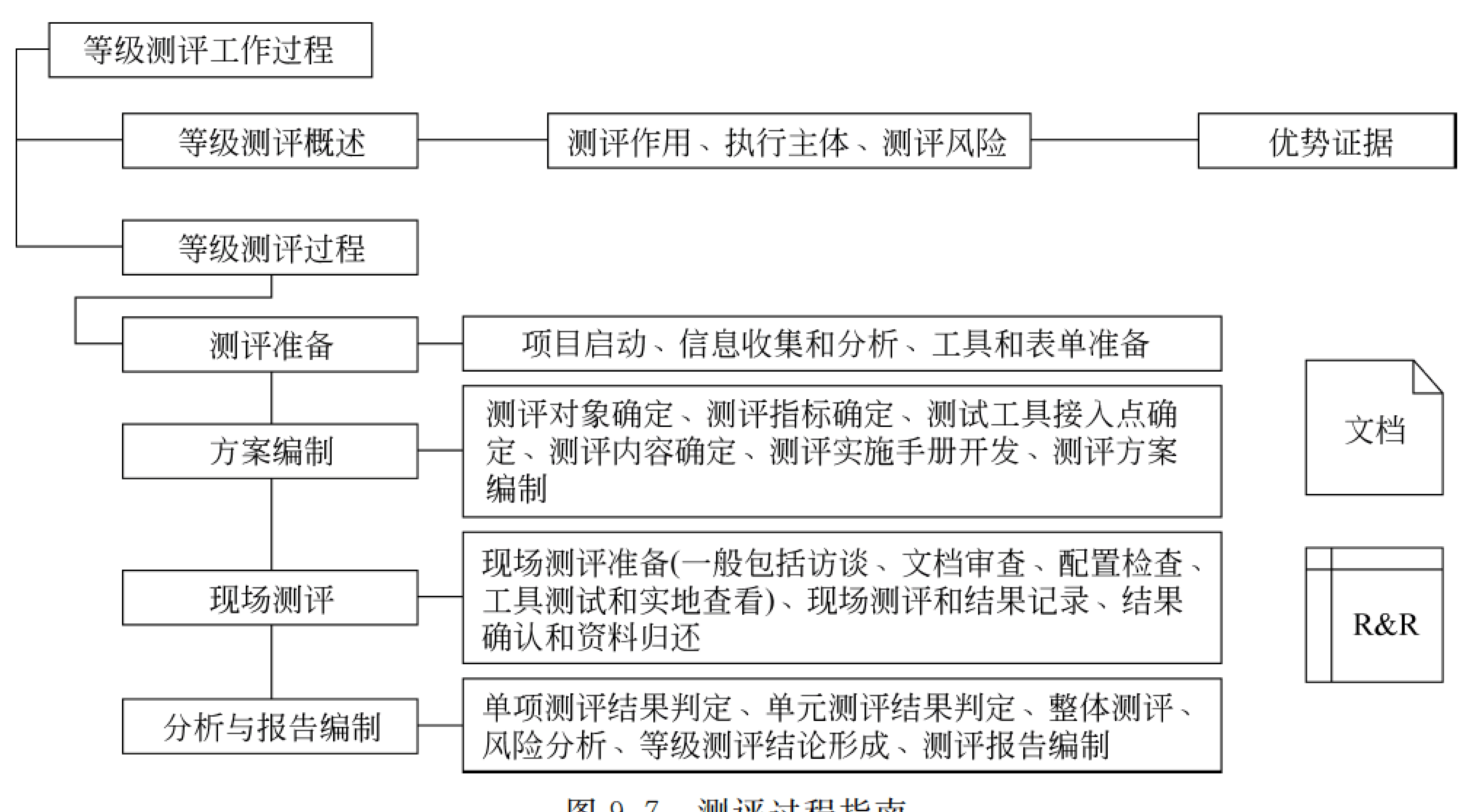


图 9.7　测评过程指南

（2）确定受侵害的客体。定级对象受到破坏时所侵害的客体包括国家安全、社会秩序、公众利益以及公民、法人和其他组织的合法权益。

侵害国家安全的事项包括以下方面：影响国家政权稳固和国防实力；影响国家统一、民族团结和社会安定；影响国家对外活动中的政治、经济利益；影响国家重要的安全保卫工作；影响国家经济竞争力和科技实力；其他影响国家安全的事项。

侵害社会秩序的事项包括以下方面：影响国家机关社会管理和公共服务的工作秩序；影响各种类型的经济活动秩序；影响各行业的科研、生产秩序；影响公众在法律约束和道德规范下的正常生活秩序等；其他影响社会秩序的事项。

影响公共利益的事项包括以下方面：影响社会成员使用公共设施；影响社会成员获取公开信息资源；影响社会成员接受公共服务等方面；其他影响公共利益的事项。

影响公民、法人和其他组织的合法权益是指由法律确认的并受法律保护的公民、法人和其他组织所享有的一定的社会权利和利益。

确定作为定级对象的信息系统受到破坏后所侵害的客体时，应首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公众利益，最后判断是否侵害公民、法人和其他组织的合法权益。

各行业可根据本行业业务特点，分析各类信息和各类信息系统与国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的关系，从而确定本行业各类信息和各类信息系统受到破坏时所侵害的客体。

（3）确定对客体的侵害程度。在客观方面，对客体的侵害外在表现为对定级对象的破坏，其危害方式表现为对信息安全的破坏和对信息系统服务的破坏，其中信息安全是指确保信息系统内信息的保密性、完整性和可用性等，系统服务安全是指确保信息系统可以及时、有效地提供服务，以完成预定的业务目标。由于业务信息安全和系统服务安全受到破坏所侵害的客体和对客体的侵害程度可能会有所不同，在定级过程中，需要分别处理这两种危害方式。

信息安全和系统服务安全受到破坏后，可能产生以下危害后果：影响行使工作职能；导致业务能力下降；引起法律纠纷；导致财务损失；造成社会不良影响；对其他组织和个人造成损失；其他影响。

（4）综合判定侵害程度。侵害程度是客观方面的不同外在表现的综合体现，因此，应首先根据不同的受侵害客体、不同危害后果分别确定其危害程度。对不同危害后果确定其危害程度所采取的方法和所考虑的角度可能不同。例如，系统服务安全被破坏导致业务能力下降的程度可以从信息系统服务覆盖的区域范围、用户人数或业务量等不同方面确定，业务信息安全被破坏导致的财物损失可以从直接的资金损失大小、间接的信息恢复费用等方面进行确定。

在针对不同的受侵害客体进行侵害程度的判断时，应参照以下不同的判别基准：

① 如果受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判断侵害程度的基准。

② 如果受侵害客体是社会秩序、公共利益或国家安全，则应以整个行业或国家的总体

利益作为判断侵害程度的基准。

不同危害后果的 3 种危害程度描述如下：

① 一般损害。工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的资产损失，有限的社会不良影响，对其他组织和个人造成较低损害。

② 严重损害。工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题、较高的资产损失、较大范围的社会不良影响，对其他组织和个人造成较严重损害。

③ 特别严重损害。工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且其功能无法执行，出现极其严重的法律问题，极高的资产损失，大范围的社会不良影响，对其他组织和个人造成非常严重损害。

信息安全和系统服务安全被破坏后对客体的侵害程度，由对不同危害结果的危害程度进行综合评定得出。由于各行业信息系统所处理的信息种类和系统服务特点各不相同，信息安全和系统服务安全受到破坏后关注的危害结果、危害程度的计算方式均可能不同，各行业可根据本行业信息特点和系统服务特点，制定危害程度的综合评定方法，并给出侵害不同客体造成损害、严重损害、特别严重损害的具体定义。

5. 确定信息系统安全保护等级

根据业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，即可得到如表 9.2 所示的业务信息系统安全保护等级。

表 9.2　信息系统安全保护等级表

使用范围	安全功能	产品类型
安全计算环境	用户身份界别	操作系统、数据库管理系统、安全审计系统、终端安全管理、身份鉴别系统等
	自主访问控制	
	系统安全审计	
	用户数据完整性保护	
	用户数据保密性保护	
	客体安全重用	
	标志与强制访问控制	
	恶意代码防范	主机防病毒等
	系统可执行程序保护	操作系统等
安全区域边界	区域边界协议过滤	安全隔离与信息交换系统、安全网关等
	区域边界安全审计	
	区域边界恶意代码防范	
	区域边界完整性保护	
	区域访问控制	

续表

使用范围	安全功能	产品类型
安全通信网络	网络安全审计	VPN、机密机、路由器等
	网络数据传输完整性保护	
	网络数据传输保密性保护	
	网络可信接入	
安全管理中心	系统管理	安全管理平台
	安全管理	
	审计管理	

9.4.4 测评过程

在等级测评工作过程中，明确规定等级测评由测评准备、方案编制、现场测评、分析与报告绘制 4 个过程，如图 9.7 所示。

1. 测评准备阶段

测评准备活动的目标是顺利启动测评项目，准备测评所需的相关资料，为顺利编制测评方案打下良好的基础。测评准备活动包括项目启动、信息收集和分析、工具和表单准备 3 项主要任务。

(1) 在项目启动任务中。测评机构组建等级测评项目组，获取测评委托单位及被测系统的基本情况，从基本资料、人员、计划安排等方面为整个等级测评项目的实施做基本准备。输入：委托测评协议书。根据测评双方签订的委托测评协议书和系统规模，测评机构组建测评项目组，从人员方面做好准备，并编制项目计划书。项目计划书应包含项目概述、工作依据、技术思路、工作内容和项目组织等。测评机构要求测评委托单位提供基本资料，包括：被测系统总体描述文件、详细描述文件、安全保护等级定级报告、系统验收报告、安全需求分析报告、安全总体方案、自查或上次等级测评报告（如果有）、测评委托单位的信息化建设状况与发展以及联络方式等。

(2) 信息收集和分析任务中。测评机构通过查阅被测系统已有资料或使用调查表格的方式，了解整个系统的构成和保护情况，为编写测评方案和开展现场测评工作奠定基础。输入：调查表格、被测系统总体描述文件、详细描述文件、安全保护等级定级报告、系统验收报告、安全需求分析报告、安全总体方案、自查或上次等级测评报告（如果有）。测评机构收集等级测评需要的各种资料，包括测评委托单位的各种方针文件、规章制度及相关过程管理记录、被测系统总体描述文件、详细描述文件、安全保护等级定级报告、安全需求分析报告、安全总体方案、安全现状评价报告、安全详细设计方案、用户指南、运行步骤、网络图表、配置管理文档等。测评机构将调查表格提交给测评委托单位，督促被测系统相关人员准确填写调查表格。测评机构收回填写完成的调查表格，并分析调查结果，了解和熟悉被测系统的实际情况。分析的内容包括被测系统的基本信息、物理位置、行业特征、管理框架、管理策略、网络及设备部署、软硬件重要性及部署情况、范围及边界、业务种类及重要性、业务流程、业务数据及重要性、业务安全保护等级、用户范围、用户类型、被测系统所处的运行环境及面临的

威胁等。这些信息可以重用自查或上次等级测评报告中的可信结果。如果调查表格填写不准确或不完善或存在相互矛盾的地方较多，测评机构应安排现场调查，与被测系统相关人员进行面对面的沟通和了解。输出/产品：填好的调查表格。

(3) 工具和表单准备任务。测评项目组成员在进行现场测评之前，应熟悉与被测系统相关的各种组件、调试测评工具、准备各种表单等。输入：各种与被测系统相关的技术资料。测评人员调试本次测评过程中将用到的测评工具，包括漏洞扫描工具、渗透性测试工具、性能测试工具和协议分析工具等。测评人员模拟被测系统搭建测评环境。准备和打印表单，主要包括现场测评授权书、文档交接单、会议记录表单。会议输出/产品：选用的测评工具清单、打印的各类表单。

2. 方案编制阶段

该阶段的目标是整理测评准备活动中获取的信息系统相关资料，为现场测评活动提供最基本的文档和指导方案。基本流程如下。

(1) 确定测评对象。识别并描述被测系统的整体结构、被测系统的边界、被测系统的网络区域、被测系统的重要节点，描述被测系统，确定并描述测评对象。

(2) 测评指标确定。根据被测系统定级结果，确定应采取的安全保护措施的 ASG 组合情况。从《信息安全技术信息系统安全等级保护基本要求》(GB/T 22239—2008)中选择相应等级的安全要求作为指标，包括：对 ASG 三类安全要求的选择；依据信息系统的组成情况，确定各个定级对象的测评指标；分别针对每个定级对象加以描述，包括系统的定级结果、指标选择两部分。

(3) 测评工具接入点确定。确定需要进行工具测试的测评对象，选择测试路径，根据测试路径确定测试工具接入点，结合网拓扑图，采用图示的方式描述测试工具的接入点、测试目的、测试用途和测试对象等相关内容。

(4) 测评内容确定。确定单元测评内容并以表格形式给出。

(5) 测评指导书开发。描述单个测评对象，包括测评对象的名称、IP 地址、用途、管理人员信息等。根据 GB/T DDDD-DDDD 的单元测评实施确定测评活动，包括测评项、测评方法、操作步骤和预期结果等四部分，并进行单元测评与整体测评。

(6) 测评方案编制。提取项目来源、测评委托单位整体信息化的建设情况及被测系统与单位其他系统之间的连接情况。根据测评实施要求，罗列所依据的标准。估算现场工作量并编制工作安排和具体测评计划，最后汇总并形成测评方案文稿，评审和提交测评方案。

3. 现场测评活动

该阶段的目标是取得分析与报告编制活动所需的、足够的证据和资料。基本流程如下。

(1) 现场测评准备。测评委托单位签署现场测评授权书。测评机构在首次会上说明具体实施内容及时间安排。双方确认需要的资源，以及确认备份过重要的数据。测评人员根据会议沟通结果，对测评结果记录表单和测评程序进行必要的更新。

(2) 现场测评和结果记录。测评结果一般包括访谈、文档审查、配置检查、工具测试、实地查看等。

(3) 结果确认和资料归还。该阶段主要完成汇总现场测评的测评记录，补充测评遗漏和需进一步验证的内容。召开测评结束会，双方确认测评过程中发现的问题。测评机构归还借阅的文档资料，由委托单位资料提供者签字确认。

4. 分析与编制报告

该阶段的目标是汇总分析测评证据，形成等级测评结论，并编制测评报告。其基本流程如下。

（1）单元测评结果判定。按层面分别汇总不同测评对象对应测评指标的单项测评结果情况，包括测评多少项、符合要求的多少项等内容，一般以表格形式列出。针对每个测评项，确定其是否为适用项。选出优势证据，并将其与要求内容的预期结果相比较。最后确认符合项、不符合项及部分符合项。

（2）整体测评。针对“部分符合”及“不符合”项，分析与之相关的其他测评项的联系。针对“部分符合”及“不符合”项，分析与之关联的其他层面的测评对象的联系。针对“部分符合”及“不符合”项，分析与之关联的其他区域的测评对象的联系。从安全角度分析被测系统整体结构的安全性，从系统角度分析被测系统整体安全防范的合理性。

（3）风险分析。结合单元与整体测评结果，判断所产生的安全问题被威胁所利用的可能性；判断被测系统的业务信息安全和系统服务安全影响程度。结合被测系统的安全保护等级对风险分析结果进行评价。

（4）等级测评结论形成。根据测评结果汇总表格，查看“不符合”项与“部分符合”项的数量，判断系统是否达到相应等级安全保护能力。

（5）测评报告编制。测评人员整理前面几项任务的输出/产品，编制测评报告相应部分。针对被测系统存在的安全隐患，提出整改建议，并编制测评报告的安全建设整改建议部分。根据现场测评的文档和记录清单，编制测评报告的单元测评的结果记录和问题分析部分。评审测评报告。评审通过后，由项目负责人签字确认并提交给测评委托单位。

9.5 本章小结

信息安全标准是确保信息安全产品和系统在设计、研发、生产、建设、使用、测评中解决其一致性、可靠性、可控性、先进性和符合性的技术规范、技术依据。统一信息安全是信息系统互联、互通、互相操作的前提。信息化的安全标准是整个安全体系不可或缺的一部分，占主要地位，这也是政府部门便于统一控制的必要手段。可以说，信息安全标准是我国信息安全保障体系的重要组成部分，也是政府进行宏观管理的重要手段。从国家的意义上来说，信息安全标准关系到国家的安全及经济利益，标准往往成为保护国家的利益、促进产业发展的一种重要手段。在信息安全面临重大问题的时候，信息安全标准化可以发挥至关重要的作用。这一安全的标准不仅仅关联国家安危，同时也关乎国家的利益，这是促使国家企业向前发展的前进动力。

第10章　信息安全法律政策和道德规范

导入语：作为一名合格的信息安全专业人员，了解一个机构的法律责任和道德义务是至关重要的。在控制机构保密和安全风险的过程中，信息安全专业人员起着重要的作用。

现代社会法律诉讼案件极为常见，有时是在民事法庭进行判决，原告可以获得较大的损失赔偿，而被告会受到惩罚。为了降低民事责任，信息安全从业者必须理解当前的法律环境，最好及时了解新的法律、规则和道德规范的发展动态。对员工和管理层进行培训，让他们懂得各自的法律责任、规则和道德规范的发展动态。对员工和管理层进行培训，让他们懂得各自的法律责任和道德义务以及如何适当地使用信息技术和信息安全技术，安全专业人员才能使整个机构朝着其首要目标努力。

本章主要知识结构如图10.1所示。

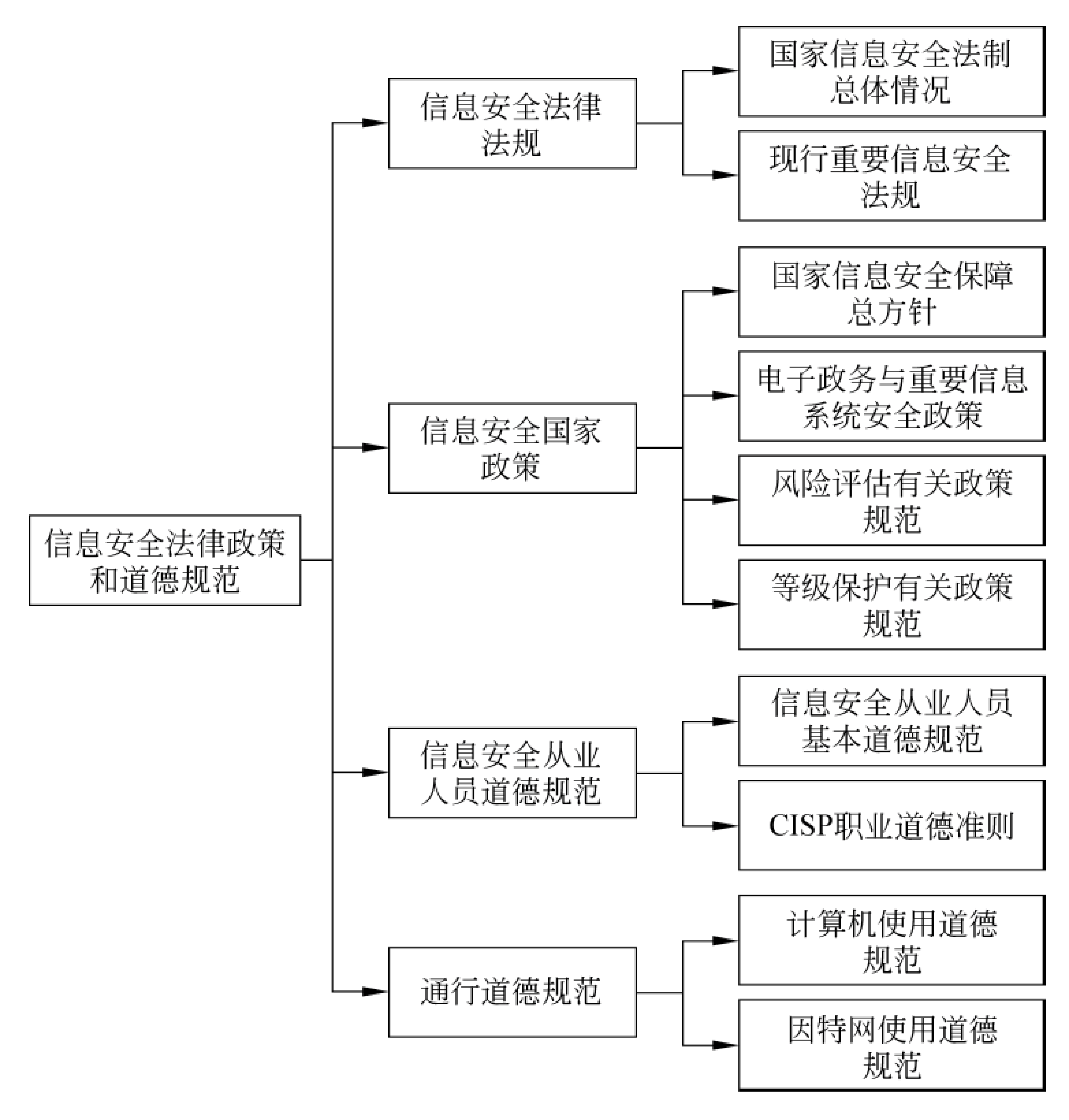


图10.1　本章主要知识结构框图

10.1 信息安全法律法规

10.1.1 国家信息安全法制总体情况

1. 法律、政策和道德的定义

法律(Law)是国家制定或认可的,由国家强制力保证实施的,以规定当事人权利和义务为内容的具有普遍约束力的社会规范。广义的法律,是指法的整体,包括法律、有法律效力的解释及行政机关为执行法律而制定的规范性文件(如规章)。狭义的法律,专指拥有立法权的国家权力机关依照立法程序制定的规范性文件。中国的十类主要部门法为宪法、行政法、民商法、刑法、经济法、诉讼法、劳动法、自然资源与环境法、军事法、科教文卫法。

政策(Policy)是指国家政权机关、政党组织和其他社会政治集团为了实现自己所代表的阶级、阶层的利益与意志,以权威形式或者标准化地规定在一定的历史时期内,应该达到的奋斗目标、遵循的行动原则、完成的明确任务、实施的工作方式、采取的一般步骤与具体措施。

道德(Ethic)是一种社会意识形态,是人们共同生活及其行为的准则和规范。道德由一定社会的经济基础所决定,并为一定的社会经济基础服务,是一种方法体系,随着阶级不同而产生变化。不同的时代、不同的阶级具有不同的道德观念。

2. 法律和政策、道德的区别

1) 法律和政策的区别

(1) 时效性。法律一旦制定,就比较稳定,长期有效,不允许经常更改。政策是针对一定的问题制定的,一旦问题解决或环境发生变化,政策就需要终止或修正。

(2) 规范性。法律具有统一的实行标准和很强的可操作性。政策只是一定的规范、原则,要实施还需要将其具体化,转换成执行细则。

(3) 公开性。法律必须是公开的,面向社会公布的。政策文件可以是公开的,也可以是"内部"的。

2) 法律和道德的区别

(1) 结构性。法律是国家意志的统一体现,有严密的逻辑体系,有不同的位阶和效力。尽管道德也可以按需分类,但不具有法律那样的严谨的结构体系。

(2) 表现性。法律都可以文字形式表现出来。道德的内容则主要存在于人们的道德意识中,表现于人们的言行上。

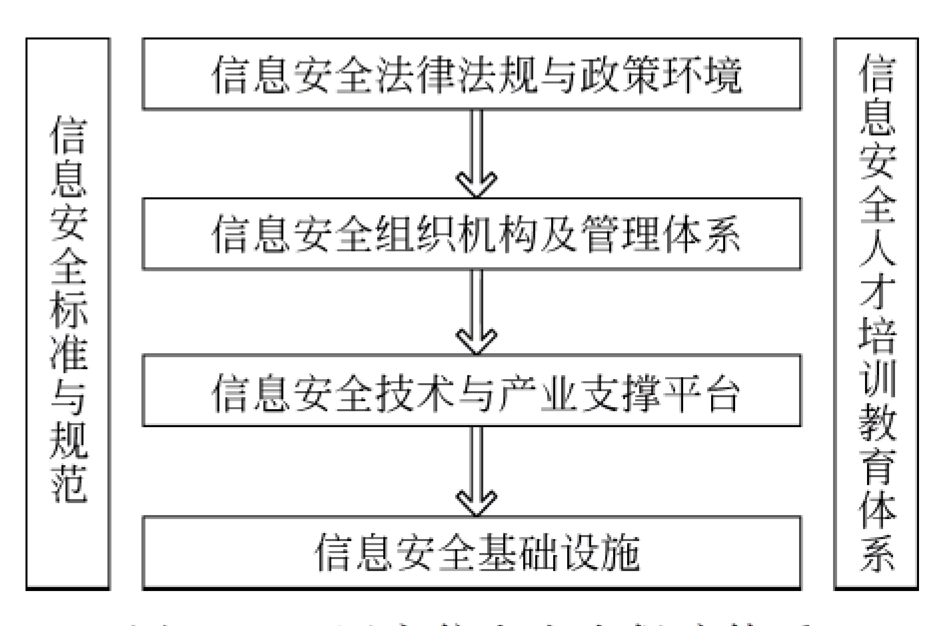


图 10.2 国家信息安全保障体系

(3) 约束性。违法犯罪的后果有明确规定,是一种"硬约束"。不道德行为的后果,是自我谴责和舆论压力,是一种"软约束"。

3. 国家信息安全法制总体情况

我国信息安全保障体系如图 10.2 所示。

(1) 信息安全在国家中的地位。

党和国家长期以来一直十分重视安全保密工作,并从敏感性、特殊性和战略性的高度,自始至

终置于党的绝对领导之下。

党的十六届四中全会将信息安全与政治安全、经济安全、文化安全并列为国家安全的重要组成要素。

(2) 我国的信息安全管理体制。

目前,我国信息安全管理格局是一个多方"齐抓共管"的体制,各相关主管部门分别执行各自的安全职能,共同维护国家的信息安全。其中包括国家信息化领导小组(国家网络与信息安全协调小组)、工信部、公安部、国家安全部、国家保密局、国家密码管理委员会等。

(3) 信息安全法治建设的意义。

信息安全法律环境是信息安全保障体系中的必要环节。明确信息安全的基本原则和基本制度、信息安全保障体系的建设、信息安全相关行为的规范、信息安全中各方权利和义务。明确违反信息安全的行为,并对其行为进行相应的处罚等。

信息安全不再只是个技术问题,而更多的是个商业和法律问题。信息安全产业的逐渐形成和成熟,需要必要的规范。信息安全法治建设涉及的主体:信息安全主管部门、各类IT产品和服务的安全(ITSP)、信息安全类产品和服务(ISSP)、信息及信息系统的拥有者和使用者。信息安全法治建设涉及的客体:信息数据、信息系统。

4. 世界各地信息安全法立法现状

信息安全法的内容相当宽泛,包括保护信息的保密性、完整性、可用性、可控性和防抵赖性的规范;有关信息主体的权利和义务的规范;保护国家利益和社会公共利益的规范等。

美国作为信息技术全球领先的超级大国,以信息为基础的国家利益遍及全球。因此,美国维护信息安全的政策与法规的目标是全球性、全方位、全领域的。

以信息为主要内容的有《电子信息自由法案》、《个人隐私保护法》、《公共信息准则》、《削减文书法》、《消费者与投资者获取信息法》、《儿童网络隐私保护法》、《电子隐私条例法案》等;以基础设施为主要内容的《1996年电信法》;以计算机安全为主要内容的《计算机保护法》、《网上电子安全法案》、《反电子盗窃法》、《计算机欺诈及滥用法案》、《网上禁赌法案》等;以电子商务为主要内容的《统一电子交易法》、《国际国内电子签名法》、《统一计算机信息交易法》、《网上贸易免税协议》等;以知识产权为主要内容的《千禧年数字版权法》、《反域名抢注消费者保护法》;还有,属于政策性文件的《国家信息基础设施行动议程》与《全球电子商务政策框架》。

纵观美国的这一系列的法律和文件,其共同具有的几个显著特点如下。

(1) 完善电子政务与信息化发展的基础环境,创造有利条件,促进发展。

(2) 排除法律上的障碍,为电子商务、电子政务等信息化建设的发展提供法律上的依据。

(3) 坚持技术中方原则,在立法上为技术发展留有空间。

(4) 针对信息技术领域乃至所有高新技术领域的所有立法都有一个共同的特点,那就是如何使千变万化、一日千里的信息技术适用单一的、稳定的法律规范。在信息化立法的过程中,政府通过积极的推进者与参与者的角色定位,积极推进信息化的发展。

欧盟自成立以来,已制定并推出了关于构建新型科技信息社会的一整套政策,如《有关实施对电信管制一揽子计划的第五份报告》、《电子通信服务的新框架》、《电子欧洲——一个面向全体欧洲人的信息社会》等政策性文件;还有《关于聚焦电信、媒体、信息技术内容及相

关规范的绿皮书》、《欧洲共同体委员会信息社会的版权和有关权利的绿皮书》等对信息化产生重大影响的规范性文件。此外，欧盟还同时出台了《促进21世纪的信息产业的长期社会发展规划》及相应的行动计划。这些政策性文件涉及因特网、电信、推行开放的通信网络、关于ISDN的数字网集成服务、卫星通信、广播频率、通信和信息服务市场、许可证制度、信息保护、税赋及电子商务等各个方面的内容。

除了这些政策性文件，欧盟还陆续发布了一系列用以规范和指导各国信息化发展的"指令"，初步建立了欧盟的信息法律体系，其中包括：《欧洲电子商务提案》、《关于数据库法律保护的指令》、《关于内部市场中与电子商务有关的若干法律问题的指令》、《协调信息社会中特定著作权和著作邻接权指令》、《著作权/出租权指令》、《远程消费保护指令》、《电信部门的隐私保护指令》、《卫星广播指令》、《软件保护指令》等。同时，欧盟的各成员国作为主权国家，在欧盟统一法律规范的指导下，根据各自的实际情况，制定了旨在促进本国信息化发展的法律规范体系，如英国2000年的《电子通信法》、爱尔兰的《电子商务法》、德国1997年的《信息与通信服务法》和《数字签名法》，意大利的《数字签名法》和2000年发布的《电子信息与文书法》等。

欧盟法律指导多成员国的法律，各成员国的法律服从和补充欧盟的法律，从而构成了由欧盟统一的法律规范和各成员国各自的法律规范两个层面的法律规范所组成的特有的法律规范体系。

纵观欧盟及欧洲各国在信息化领域的政策法律环境，除前文已经概括的与美国的信息政策环境相同的一些特点，如完善电子政务与信息化发展的基础环境、排除法律障碍、坚持技术中立原则、注重全球一体化原则外，欧盟及欧洲各国还具备以下几个方面的较为突出的特点。

(1) 采取注重欧盟整体信息化推进、法制统一与充分发挥各国特长和优势相结合的原则，从不同角度推进信息化的发展。

(2) 利用欧洲一体化的优势，协调各国的法制环境，为信息化与贸易、交流等创造无障碍的法制环境。

(3) 重视信息化发展过程中信息服务内容的管制和净化。例如，针对信息提供商(ISP)，很多欧洲国家都采取了较为严格管制的态度。当在ISP的法律责任问题上，特别是有人在ISP提供的主页空间上有侵犯他人的知识产权、名誉权等行为时ISP究竟要不要承担连带责任问题上，欧盟与美国的态度差距很大。欧盟采取的是相对严格的责任原则，而美国则更多地运用了非严格即宽松的责任追究制度。例如，美国在其《数字千年版权法》中，规定ISP在收到权利人的通知后，及时关闭其服务器上客户的侵权网页就不用承担法律责任，但是该法对如果ISP没有做出相应的行动是否要承担责任并没有做出具体的规定。相比之下，欧盟则严厉得多，如果ISP在接到权利人的通知之后不立即做出有效行动关闭侵权网站，就会承担法律责任；有的成员国甚至规定ISP必须及时把侵权者的有关信息提供给权利人。

在英国，1996年9月颁布了《三R互联网络安全规则》，用于规定消除网络中的非法资料的内容。其基本措施为"分级认定、举报告发、责任承担"，即3R(以上三项的英文词头)。此后，英国政府于1999年9月发布工作计划，提出将由政府带头发展方便且容易使用的过滤技术，以保护公民免受网络有害内容的侵害。

在法国，1997 年 3 月提出《互联网宪章》，将“明显非法的网络内容及行为”定义为：“明显有悖于公共秩序的内容或行为，如对儿童进行性引诱、煽动种族仇恨、教唆谋杀、作淫媒以及毒品交易及危害国家安全等；对敏感内容定义为：并不明显违法，但实质上对某些人造成伤害的内容。

重视网络隐私权的保护。欧盟对于网络隐私权保护的框架文件有 4 个：一个是为配合经合组织的《关于隐私和个人资料的跨国境流动的保护指引》制定的《关于在自动运行系统中个人资料保护公约》；二是 1995 年通过，1998 年 10 月生效的《关于个人资料的运行和自由流动的保护指令》；三是 1997 年 7 月欧委会个人资料保护工作组制定的《关于个人资料向第三国传递的第一个指导——评估充分性的可能方案》；四是 1999 年部长会议关于互联网隐私保护指引备忘录中规定的《关于在信息高速公路上收集和传送个人资料的保护》。

俄罗斯信息基础设施尚不发达，信息的利用正处于发展之中。因此，俄罗斯维护信息安全的政策与措施的基本目标，是为发展以信息为基础的各方面事业创造良好条件，防止外部和内部敌对势力破坏。

早在 1994 年俄罗斯就通过了信息安全保护法——《政府通信和信息联邦机构法》，在俄罗斯宪法中，还明确界定了信息资源开放和保密的范畴，提出了保护信息的法律责任。另外，针对信息安全保护的法规还有《数字签名法》、《信息化和信息保护法》、《国家秘密法》、《信息保护设备认证法》以及针对加密设备的研制、生产、实现和应用的法规等。统领全局的《国家信息安全学说》于 2000 年获批，该学说明确了俄罗斯在信息领域的利益，为俄罗斯制定了许多确保俄罗斯国家安全和公民权利的具体措施，是制定和起草其他有关信息安全保障国家政策、法律、提案和专门计划的基础。

针对目前面临的国家信息资源废除垄断、国家信息网络集成化和信息交换非集中化过程，俄罗斯还制定系列与《国家信息安全学说》相适应的文件、标准和方法，并指定特派机构制定专业技术规范以调整现有法律体系，加入针对行业和部门的信息保护政策。2003 年推出的《技术调整法》还专门就安全性技术调整、知识产权和著作权做了翔实的说明。

为了推动信息产业化的发展，俄联邦政府批准了《2002—2010 年电子俄罗斯》专项纲要，为国家信息安全保障提供完整的法律体系和适宜的调整机制。

日本的信息技术水平和信息化程度仅次于美国，其从国家整体发展战略的高度建构信息安全体系。在出台有关发展战略构想的同时，日本全面重视信息安全立法工作，制定了一系列相关的法律和法规。

2000 年出台《防止非法接入法》以建立防止和刑事处罚非法接入或属于这种行为的活动规章，同年的《电子签名：鉴别法》对电子签名的有效性作了详细规定，依据国际通用测评认证标准修订的《电子商务网络安全对策指南》则进一步健全了电子商务的安全管理机制。另外针对信息电子证书的需要，还对《商业登记法》作了修订。

为避免关键基础设施遭受计算机恐怖活动攻击，日本政府推出了《关于防范关键基础设施计算机恐怖活动的特别行动计划》。《日本信息安全指导方针》是为日本电子政府计划作了全面规划，而《确保电子政务实施过程中的信息安全行动方案》则保证电子政务的安全。

在我国，1994 年 2 月 18 日，国务院颁布了《中华人民共和国计算机信息系统安全保护条例》，这是一个标志性的、基础性的法规。到目前为止，我国信息安全的法律体系可分为 4 个层面：

(1) 一般性法律规定。这些法律法规并没有专门对信息安全进行规定，但是这些法律法规所规范和约束的对象包括涉及信息安全的行为，如宪法、国家安全法、国家秘密法、治安管理处罚条例等。

(2) 规范和惩罚信息网络犯罪的法律。这类法律包括《中华人民共和国刑法》、《全国人大常委会关于维护互联网安全的决定》等。

(3) 直接针对信息安全的特别规定。这类法律法规主要有《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》、《中华人民共和国电信条例》等。

(4) 具体规范信息安全技术、信息安全管理等方面的规定。这类法律法规主要有《商用密码管理条例》、《计算机病毒防治管理办法》、《计算机信息系统国际联网保密管理规定》、《金融机构计算机信息系统安全保护工作暂行规定》等。此外，还有一些地方性法规和规章。

我国虽然制定了许多有关信息安全方面的法律法规，但是总体上我国的信息安全立法还处于起步阶段，具体体现在以下几个方面。

(1) 还没有形成一个完整性、适用性、针对性的完善的法律体系。现有法律法规仅仅调整某一个方面的问题，缺少综合性的信息安全法作为主导，使之相互呼应形成体系因而在实践中造成多环节、多部门分割管理的状况，这在一定程度上造成了法律资源的严重浪费，同时也说明了我国现行的信息安全法律基本上还处于法规规章的层次上，在法律层面上的信息安全立法还比较少且很不完善。

(2) 不具开放性。法律结构比较单一、层次较低，难以适应信息网络技术发展的需要和不断出现的信息安全问题。

(3) 缺乏兼容性。我国的信息安全法律法规存在着许多难以同传统的法律原则、法律规范协调的地方。

(4) 难以操作。如果一部法律难以操作，那么该法律就难以起到应有的规范约束作用。我国的安全法律中就存在着这些问题，如同一行为有多个行政处罚主体、不同法律规定的处罚幅度不一致、行政审批部门及审批事项多等。

10.1.2 现行重要信息安全法规

党中央、国务院对我国的信息安全问题高度重视，先后发布实施了一系列规范性文件，就新形势下如何开展和加强我国信息安全的防范和处置工作提出了前瞻要求，进行了具体部署，并指出要建立行业主管和协管部门紧密配合的网络管理机制，完善法律法规，依法加强管理，探索建立互联网管理的长效机制。根据党中央、国务院有关文件精神，起草并制定信息安全的相关法律是建立我国信息安全监督管理长效机制的重要保障。

下面为大家介绍几部现行的重要的信息安全的法律和相关法规。

1.《保守国家秘密法》

第一章　总则

第一条　为了保守国家秘密，维护国家安全和利益，保障改革开放和社会主义建设事业的顺利进行，制定本法。

第二条　国家秘密是关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。

第三条　国家秘密受法律保护。一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务。任何危害国家秘密安全的行为，都必须受到法律追究。

第四条　保守国家秘密的工作（以下简称保密工作），实行积极防范、突出重点、依法管理的方针，既确保国家秘密安全，又便利信息资源合理利用。法律、行政法规规定公开的事项，应当依法公开。

第五条　国家保密行政管理部门主管全国的保密工作。县级以上地方各级保密行政管理部门主管本行政区域的保密工作。

第六条　国家机关和涉及国家秘密的单位（以下简称机关、单位）管理本机关和本单位的保密工作。中央国家机关在其职权范围内，管理或者指导本系统的保密工作。

第七条　机关、单位应当实行保密工作责任制，健全保密管理制度，完善保密防护措施，开展保密宣传教育，加强保密检查。

第八条　国家对在保守、保护国家秘密以及改进保密技术、措施等方面成绩显著的单位或者个人给予奖励。

第二章　国家秘密的范围和密级

第九条　下列涉及国家安全和利益的事项，泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，应当确定为国家秘密：

（一）国家事务重大决策中的秘密事项。

（二）国防建设和武装力量活动中的秘密事项。

（三）外交和外事活动中的秘密事项以及对外承担保密义务的秘密事项。

（四）国民经济和社会发展中的秘密事项。

（五）科学技术中的秘密事项。

（六）维护国家安全活动和追查刑事犯罪中的秘密事项。

（七）经国家保密行政管理部门确定的其他秘密事项。

政党的秘密事项中符合前款规定的，属于国家秘密。

第十条　国家秘密的密级分为绝密、机密、秘密三级。

绝密级国家秘密是最重要的国家秘密，泄露会使国家安全和利益遭受特别严重的损害；机密级国家秘密是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害；秘密级国家秘密是一般的国家秘密，泄露会使国家安全和利益遭受损害。

第十一条　国家秘密及其密级的具体范围，由国家保密行政管理部门分别会同外交、公安、国家安全和其他中央有关机关规定。军事方面的国家秘密及其密级的具体范围，由中央军事委员会规定。国家秘密及其密级的具体范围的规定，应当在有关范围内公布，并根据情况变化及时调整。

第十二条　机关、单位负责人及其指定的人员为定密责任人，负责本机关、本单位的国家秘密确定、变更和解除工作。机关、单位确定、变更和解除本机关、本单位的国家秘密，应当由承办人提出具体意见，经定密责任人审核批准。

第十三条　确定国家秘密的密级，应当遵守定密权限。

中央国家机关、省级机关及其授权的机关、单位可以确定绝密级、机密级和秘密级国家秘密；设区的市、自治州一级的机关及其授权的机关、单位可以确定机密级和秘密级国家秘密。具体的定密权限、授权范围由国家保密行政管理部门规定。机关、单位执行上级确定的

国家秘密事项，需要定密的，根据所执行的国家秘密事项的密级确定。下级机关、单位认为本机关、本单位产生的有关定密事项属于上级机关、单位的定密权限，应当先行采取保密措施，并立即报请上级机关、单位确定；没有上级机关、单位的，应当立即提请有相应定密权限的业务主管部门或者保密行政管理部门确定。公安、国家安全机关在其工作范围内按照规定的权限确定国家秘密的密级。

第十四条　机关、单位对所产生的国家秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级，同时确定保密期限和知悉范围。

第十五条　国家秘密的保密期限，应当根据事项的性质和特点，按照维护国家安全和利益的需要，限定在必要的期限内；不能确定期限的，应当确定解密的条件。

国家秘密的保密期限，除另有规定外，绝密级不超过 30 年，机密级不超过 20 年，秘密级不超过 10 年。

机关、单位应当根据工作需要，确定具体的保密期限、解密时间或者解密条件。

机关、单位对在决定和处理有关事项工作过程中确定需要保密的事项，根据工作需要决定公开的，正式公布时即视为解密。

第十六条　国家秘密的知悉范围，应当根据工作需要限定在最小范围。

国家秘密的知悉范围能够限定到具体人员的，限定到具体人员；不能限定到具体人员的，限定到机关、单位，由机关、单位限定到具体人员。

国家秘密的知悉范围以外的人员，因工作需要知悉国家秘密的，应当经过机关、单位负责人批准。

第十七条　机关、单位对承载国家秘密的纸介质、光介质、电磁介质等载体（以下简称国家秘密载体）以及属于国家秘密的设备、产品，应当做出国家秘密标志。

不属于国家秘密的，不应当做出国家秘密标志。

第十八条　国家秘密的密级、保密期限和知悉范围，应当根据情况变化及时变更。国家秘密的密级、保密期限和知悉范围的变更，由原定密机关、单位决定，也可以由其上级机关决定。

国家秘密的密级、保密期限和知悉范围变更的，应当及时书面通知知悉范围内的机关、单位或者人员。

第十九条　国家秘密的保密期限已满的，自行解密。

机关、单位应当定期审核所确定的国家秘密。对在保密期限内因保密事项范围调整不再作为国家秘密事项，或者公开后不会损害国家安全和利益，不需要继续保密的，应当及时解密；对需要延长保密期限的，应当在原保密期限届满前重新确定保密期限。提前解密或者延长保密期限的，由原定密机关、单位决定，也可以由其上级机关决定。

第二十条　机关、单位对是否属于国家秘密或者属于何种密级不明确或者有争议的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门确定。

第三章　保密制度

第二十一条　国家秘密载体的制作、收发、传递、使用、复制、保存、维修和销毁，应当符合国家保密规定。

绝密级国家秘密载体应当在符合国家保密标准的设施、设备中保存，并指定专人管理；未经原定密机关、单位或者其上级机关批准，不得复制和摘抄；收发、传递和外出携带，应当

指定人员负责,并采取必要的安全措施。

第二十二条　属于国家秘密的设备、产品的研制、生产、运输、使用、保存、维修和销毁,应当符合国家保密规定。

第二十三条　存储、处理国家秘密的计算机信息系统(以下简称涉密信息系统)按照涉密程度实行分级保护。

涉密信息系统应当按照国家保密标准配备保密设施、设备。保密设施、设备应当与涉密信息系统同步规划,同步建设,同步运行。

涉密信息系统应当按照规定,经检查合格后,方可投入使用。

第二十四条　机关、单位应当加强对涉密信息系统的管理,任何组织和个人不得有下列行为:

(一)将涉密计算机、涉密存储设备接入互联网及其他公共信息网络。

(二)在未采取防护措施的情况下,在涉密信息系统与互联网及其他公共信息网络之间进行信息交换。

(三)使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息。

(四)擅自卸载、修改涉密信息系统的安全技术程序、管理程序。

(五)将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或者改作其他用途。

第二十五条　机关、单位应当加强对国家秘密载体的管理,任何组织和个人不得有下列行为:

(一)非法获取、持有国家秘密载体。

(二)买卖、转送或者私自销毁国家秘密载体。

(三)通过普通邮政、快递等无保密措施的渠道传递国家秘密载体。

(四)邮寄、托运国家秘密载体出境。

(五)未经有关主管部门批准,携带、传递国家秘密载体出境。

第二十六条　禁止非法复制、记录、存储国家秘密。

禁止在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密。

禁止在私人交往和通信中涉及国家秘密。

第二十七条　报刊、图书、音像制品、电子出版物的编辑、出版、印制、发行,广播节目、电视节目、电影的制作和播放,互联网、移动通信网等公共信息网络及其他传媒的信息编辑、发布,应当遵守有关保密规定。

第二十八条　互联网及其他公共信息网络运营商、服务商应当配合公安机关、国家安全机关、检察机关对泄密案件进行调查;发现利用互联网及其他公共信息网络发布的信息涉及泄露国家秘密的,应当立即停止传输,保存有关记录,向公安机关、国家安全机关或者保密行政管理部门报告;应当根据公安机关、国家安全机关或者保密行政管理部门的要求,删除涉及泄露国家秘密的信息。

第二十九条　机关、单位公开发布信息以及对涉及国家秘密的工程、货物、服务进行采购时,应当遵守保密规定。

第三十条　机关、单位对外交往与合作中需要提供国家秘密事项,或者任用、聘用的境

外人员因工作需要知悉国家秘密的，应当报国务院有关主管部门或者省、自治区、直辖市人民政府有关主管部门批准，并与对方签订保密协议。

第三十一条　举办会议或者其他活动涉及国家秘密的，主办单位应当采取保密措施，并对参加人员进行保密教育，提出具体保密要求。

第三十二条　机关、单位应当将涉及绝密级或者较多机密级、秘密级国家秘密的机构确定为保密要害部门，将集中制作、存放、保管国家秘密载体的专门场所确定为保密要害部位，按照国家保密规定和标准配备、使用必要的技术防护设施、设备。

第三十三条　军事禁区和属于国家秘密不对外开放的其他场所、部位，应当采取保密措施，未经有关部门批准，不得擅自决定对外开放或者扩大开放范围。

第三十四条　从事国家秘密载体制作、复制、维修、销毁，涉密信息系统集成，或者武器装备科研生产等涉及国家秘密业务的企业事业单位，应当经过保密审查，具体办法由国务院规定。

机关、单位委托企业事业单位从事前款规定的业务，应当与其签订保密协议，提出保密要求，采取保密措施。

第三十五条　在涉密岗位工作的人员（以下简称涉密人员），按照涉密程度分为核心涉密人员、重要涉密人员和一般涉密人员，实行分类管理。任用、聘用涉密人员应当按照有关规定进行审查。涉密人员应当具有良好的政治素质和品行，具有胜任涉密岗位所要求的工作能力。涉密人员的合法权益受法律保护。

第三十六条　涉密人员上岗应当经过保密教育培训，掌握保密知识技能，签订保密承诺书，严格遵守保密规章制度，不得以任何方式泄露国家秘密。

第三十七条　涉密人员出境应当经有关部门批准，有关机关认为涉密人员出境将对国家安全造成危害或者对国家利益造成重大损失的，不得批准出境。

第三十八条　涉密人员离岗离职实行脱密期管理。涉密人员在脱密期内，应当按照规定履行保密义务，不得违反规定就业，不得以任何方式泄露国家秘密。

第三十九条　机关、单位应当建立健全涉密人员管理制度，明确涉密人员的权利、岗位责任和要求，对涉密人员履行职责情况开展经常性的监督检查。

第四十条　国家工作人员或者其他公民发现国家秘密已经泄露或者可能泄露时，应当立即采取补救措施并及时报告有关机关、单位。机关、单位接到报告后，应当立即作出处理，并及时向保密行政管理部门报告。

第四章　监督管理

第四十一条　国家保密行政管理部门依照法律、行政法规的规定，制定保密规章和国家保密标准。

第四十二条　保密行政管理部门依法组织开展保密宣传教育、保密检查、保密技术防护和泄密案件查处工作，对机关、单位的保密工作进行指导和监督。

第四十三条　保密行政管理部门发现国家秘密确定、变更或者解除不当的，应当及时通知有关机关、单位予以纠正。

第四十四条　保密行政管理部门对机关、单位遵守保密制度的情况进行检查，有关机关、单位应当配合。保密行政管理部门发现机关、单位存在泄密隐患的，应当要求其采取措施，限期整改；对存在泄密隐患的设施、设备、场所，应当责令停止使用；对严重违反保密规定

的涉密人员，应当建议有关机关、单位给予处分并调离涉密岗位；发现涉嫌泄露国家秘密的，应当督促、指导有关机关、单位进行调查处理。涉嫌犯罪的，移送司法机关处理。

第四十五条　保密行政管理部门对保密检查中发现的非法获取、持有的国家秘密载体，应当予以收缴。

第四十六条　办理涉嫌泄露国家秘密案件的机关，需要对有关事项是否属于国家秘密以及属于何种密级进行鉴定的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门鉴定。

第四十七条　机关、单位对违反保密规定的人员不依法给予处分的，保密行政管理部门应当建议纠正，对拒不纠正的，提请其上一级机关或者监察机关对该机关、单位负有责任的领导人员和直接责任人员依法予以处理。

第五章　法律责任

第四十八条　违反本法规定，有下列行为之一的，依法给予处分；构成犯罪的，依法追究刑事责任：

（一）非法获取、持有国家秘密载体的。

（二）买卖、转送或者私自销毁国家秘密载体的。

（三）通过普通邮政、快递等无保密措施的渠道传递国家秘密载体的。

（四）邮寄、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传递国家秘密载体出境的。

（五）非法复制、记录、存储国家秘密的。

（六）在私人交往和通信中涉及国家秘密的。

（七）在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密的。

（八）将涉密计算机、涉密存储设备接入互联网及其他公共信息网络的。

（九）在未采取防护措施的情况下，在涉密信息系统与互联网及其他公共信息网络之间进行信息交换的。

（十）使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息的。

（十一）擅自卸载、修改涉密信息系统的安全技术程序、管理程序的。

（十二）将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或者改作其他用途的。

有前款行为尚不构成犯罪，且不适用处分的人员，由保密行政管理部门督促其所在机关、单位予以处理。

第四十九条　机关、单位违反本法规定，发生重大泄密案件的，由有关机关、单位依法对直接负责的主管人员和其他直接责任人员给予处分；不适用处分的人员，由保密行政管理部门督促其主管部门予以处理。

机关、单位违反本法规定，对应当定密的事项不定密，或者对不应当定密的事项定密，造成严重后果的，由有关机关、单位依法对直接负责的主管人员和其他直接责任人员给予处分。

第五十条　互联网及其他公共信息网络运营商、服务商违反本法第二十八条规定的，由公安机关或者国家安全机关、信息产业主管部门按照各自职责分工依法予以处罚。

第五十一条　保密行政管理部门的工作人员在履行保密管理职责中滥用职权、玩忽职守、徇私舞弊的，依法给予处分；构成犯罪的，依法追究刑事责任。

第六章　附则

第五十二条　中央军事委员会根据本法制定中国人民解放军保密条例。

第五十三条　本法自 2010 年 10 月 1 日起施行。

2.《电子签名法》

第一章　总则

第一条　为了规范电子签名行为，确立电子签名的法律效力，维护有关各方的合法权益，制定本法。

第二条　本法所称电子签名，是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。本法所称数据电文，是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。

第三条　民事活动中的合同或者其他文件、单证等文书，当事人可以约定使用或者不使用电子签名、数据电文。当事人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否定其法律效力。前款规定不适用下列文书：

（一）涉及婚姻、收养、继承等人身关系的。

（二）涉及土地、房屋等不动产权益转让的。

（三）涉及停止供水、供热、供气、供电等公用事业服务的。

（四）法律、行政法规规定的不适用电子文书的其他情形。

第二章　数据电文

第四条　能够有形地表现所载内容，并可以随时调取查用的数据电文，视为符合法律、法规要求的书面形式。

第五条　符合下列条件的数据电文，视为满足法律、法规规定的原件形式要求：

（一）能够有效地表现所载内容并可供随时调取查用。

（二）能够可靠地保证自最终形成时起，内容保持完整、未被更改。但是，在数据电文上增加背书以及数据交换、储存和显示过程中发生的形式变化不影响数据电文的完整性。

第六条　符合下列条件的数据电文，视为满足法律、法规规定的文件保存要求：

（一）能够有效地表现所载内容并可供随时调取查用。

（二）数据电文的格式与其生成、发送或者接收时的格式相同，或者格式不相同但是能够准确表现原来生成、发送或者接收的内容。

（三）能够识别数据电文的发件人、收件人以及发送、接收的时间。

第七条　数据电文不得仅因为其是以电子、光学、磁或者类似手段生成、发送、接收或者储存的而被拒绝作为证据使用。

第八条　审查数据电文作为证据的真实性，应当考虑以下因素：

（一）生成、储存或者传递数据电文方法的可靠性。

（二）保持内容完整性方法的可靠性。

（三）用以鉴别发件人方法的可靠性。

（四）其他相关因素。

第九条　数据电文有下列情形之一的，视为发件人发送：

（一）经发件人授权发送的。

（二）发件人的信息系统自动发送的。

（三）收件人按照发件人认可的方法对数据电文进行验证后结果相符的。当事人对前款规定的事项另有约定的，从其约定。

第十条　法律、行政法规规定或者当事人约定数据电文需要确认收讫的，应当确认收讫。发件人收到收件人的收讫确认时，数据电文视为已经收到。

第十一条　数据电文进入发件人控制之外的某个信息系统的时间，视为该数据电文的发送时间。收件人指定特定系统接收数据电文的，数据电文进入该特定系统的时间，视为该数据电文的接收时间；未指定特定系统的，数据电文进入收件人的任何系统的首次时间，视为该数据电文的接收时间。当事人对数据电文的发送时间、接收时间另有约定的，从其约定。

第十二条　发件人的主营业地为数据电文的发送地点，收件人的主营业地为数据电文的接收地点。没有主营业地的，其经常居住地为发送或者接收地点。当事人对数据电文的发送地点、接收地点另有约定的，从其约定。

第三章　电子签名与认证

第十三条　电子签名同时符合下列条件的，视为可靠的电子签名：

（一）电子签名制作数据用于电子签名时，属于电子签名人专有。

（二）签署时电子签名制作数据仅由电子签名人控制。

（三）签署后对电子签名的任何改动能够被发现。

（四）签署后对数据电文内容和形式的任何改动能够被发现。当事人也可以选择使用符合其约定的可靠条件的电子签名。

第十四条　可靠的电子签名与手写签名或者盖章具有同等的法律效力。

第十五条　电子签名人应当妥善保管电子签名制作数据。电子签名人知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知有关各方，并终止使用该电子签名制作数据。

第十六条　电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。

第十七条　提供电子认证服务，应当具备下列条件：

（一）具有与提供电子认证服务相适应的专业技术人员和管理人员。

（二）具有与提供电子认证服务相适应的资金和经营场所。

（三）具有符合国家安全标准的技术和设备。

（四）具有国家密码管理机构同意使用密码的证明文件。

（五）法律、行政法规规定的其他条件。

第十八条　从事电子认证服务，应当向国务院信息产业主管部门提出申请，并提交符合本法第十七条规定条件的相关材料。国务院信息产业主管部门接到申请后经依法审查，征求国务院商务主管部门等有关部门的意见后，自接到申请之日起 45 日内作出许可或者不予许可的决定。予以许可的，颁发电子认证许可证书；不予许可的，应当书面通知申请人并告知理由。申请人应当持电子认证许可证书依法向工商行政管理部门办理企业登记手续。取得认证资格的电子认证服务提供者，应当按照国务院信息产业主管部门的规定在互联网上

公布其名称、许可证号等信息。

第十九条　电子认证服务提供者应当制定、公布符合国家有关规定的电子认证业务规则，并向国务院信息产业主管部门备案。电子认证业务规则应当包括责任范围、作业操作规范、信息安全保障措施等事项。

第二十条　电子签名人向电子认证服务提供者申请电子签名认证证书，应当提供真实、完整和准确的信息。电子认证服务提供者收到电子签名认证证书申请后，应当对申请人的身份进行查验，并对有关材料进行审查。

第二十一条　电子认证服务提供者签发的电子签名认证证书应当准确无误，并应当载明下列内容：

（一）电子认证服务提供者名称。

（二）证书持有人名称。

（三）证书序列号。

（四）证书有效期。

（五）证书持有人的电子签名验证数据。

（六）电子认证服务提供者的电子签名。

（七）国务院信息产业主管部门规定的其他内容。

第二十二条　电子认证服务提供者应当保证电子签名认证证书内容在有效期内完整、准确，并保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项。

第二十三条　电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止服务 90 日前，就业务承接及其他有关事项通知有关各方。电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止服务 60 日前向国务院信息产业主管部门报告，并与其他电子认证服务提供者就业务承接进行协商，作出妥善安排。电子认证服务提供者未能就业务承接事项与其他电子认证服务提供者达成协议的，应当申请国务院信息产业主管部门安排其他电子认证服务提供者承接其业务。

电子认证服务提供者被依法吊销电子认证许可证书的，其业务承接事项的处理按照国务院信息产业主管部门的规定执行。

第二十四条　电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后 5 年。

第二十五条　国务院信息产业主管部门依照本法制定电子认证服务业的具体管理办法，对电子认证服务提供者依法实施监督管理。

第二十六条　经国务院信息产业主管部门根据有关协议或者对等原则核准后，中华人民共和国境外的电子认证服务提供者在境外签发的电子签名认证证书与依照本法设立的电子认证服务提供者签发的电子签名认证证书具有同等的法律效力。

第四章　法律责任

第二十七条　电子签名人知悉电子签名制作数据已经失密或者可能已经失密未及时告知有关各方、并终止使用电子签名制作数据，未向电子认证服务提供者提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、电子认证服务提供者造成损失的，承担赔偿责任。

第二十八条　电子签名人或者电子签名依赖方因依据电子认证服务提供者提供的电子签名认证服务从事民事活动遭受损失，电子认证服务提供者不能证明自己无过错的，承担赔偿责任。

第二十九条　未经许可提供电子认证服务的，由国务院信息产业主管部门责令停止违法行为；有违法所得的，没收违法所得；违法所得 30 万元以上的，处违法所得一倍以上 3 倍以下的罚款；没有违法所得或者违法所得不足 30 万元的，处十万元以上 30 万元以下的罚款。

第三十条　电子认证服务提供者暂停或者终止电子认证服务，未在暂停或者终止服务 60 日前向国务院信息产业主管部门报告的，由国务院信息产业主管部门对其直接负责的主管人员处 1 万元以上 5 万元以下的罚款。

第三十一条　电子认证服务提供者不遵守认证业务规则、未妥善保存与认证相关的信息，或者有其他违法行为的，由国务院信息产业主管部门责令限期改正；逾期未改正的，吊销电子认证许可证书，其直接负责的主管人员和其他直接责任人员 10 年内不得从事电子认证服务。吊销电子认证许可证书的，应当予以公告并通知工商行政管理部门。

第三十二条　伪造、冒用、盗用他人的电子签名，构成犯罪的，依法追究刑事责任；给他人造成损失的，依法承担民事责任。

第三十三条　依照本法负责电子认证服务业监督管理工作的部门的工作人员，不依法履行行政许可、监督管理职责的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第五章　附则

第三十四条　本法中下列用语的含义：

（一）电子签名人，是指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人。

（二）电子签名依赖方，是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。

（三）电子签名认证证书，是指可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录。

（四）电子签名制作数据，是指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。

（五）电子签名验证数据，是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。

第三十五条　国务院或者国务院规定的部门可以依据本法制定政务活动和其他社会活动中使用电子签名、数据电文的具体办法。

第三十六条　本法自 2005 年 4 月 1 日起施行。

本法律法规被称为“中国首部真正意义上的信息化法律”，自此电子签名与传统手写签名和盖章具有同等的法律效力。《电子签名法》是我国推进电子商务发展、扫除电子商务发展障碍的重要步骤。虽然舆论普遍认为《电子签名法》将会极大地促进电子商务在我国的快速发展，但在网络交易安全、相关法律衔接等“拦路虎”面前，有关专家认为，现阶段《电子签名法》的标志意义大于实际意义。

3.《刑法》有关信息安全犯罪的规定

第二百八十五条　违反国家规定,侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的,处3年以下有期徒刑或者拘役。违反国家规定,侵入前款规定以外的计算机信息系统或者采用其他技术手段,获取该计算机信息系统中存储、处理或者传输的数据,或者对该计算机信息系统实施非法控制,情节严重的,处3年以下有期徒刑或者拘役,并处或者单处罚金;情节特别严重的,处3年以上7年以下有期徒刑,并处罚金。提供专门用于侵入、非法控制计算机信息系统的程序、工具,或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具,情节严重的,依照前款的规定处罚。

第二百八十六条　违反国家规定,对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行,后果严重的,处5年以下有期徒刑或者拘役;后果特别严重的,处5年以上有期徒刑。违反国家规定,对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作,后果严重的,依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,后果严重的,依照第一款的规定处罚。

第二百八十七条　利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的,依照本法有关规定定罪处罚。

4.《全国人大常委会关于维护互联网安全的决定》

我国的互联网,在国家大力倡导和积极推动下,在经济建设和各项事业中得到日益广泛的应用,使人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化,对于加快我国国民经济、科学技术的发展和社会服务信息化进程具有重要作用。同时,如何保障互联网的运行安全和信息安全问题已经引起全社会的普遍关注。为了兴利除弊,促进我国互联网的健康发展,维护国家安全和社会公共利益,保护个人、法人和其他组织的合法权益,特作以下决定:

为了保障互联网的运行安全,对有下列行为之一,构成犯罪的,依照刑法有关规定追究刑事责任:

(1) 侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统。

(2) 故意制作、传播计算机病毒等破坏性程序,攻击计算机系统及通信网络,致使计算机系统及通信网络遭受损害。

(3) 违反国家规定,擅自中断计算机网络或者通信服务,造成计算机网络或者通信系统不能正常运行。

为了维护国家安全和社会稳定,对有下列行为之一,构成犯罪的,依照刑法有关规定追究刑事责任:

(1) 利用互联网造谣、诽谤或者发表、传播其他有害信息,煽动颠覆国家政权、推翻社会主义制度,或者煽动分裂国家、破坏国家统一。

(2) 通过互联网窃取、泄露国家秘密、情报或者军事秘密。

(3) 利用互联网煽动民族仇恨、民族歧视,破坏民族团结。

(4) 利用互联网组织邪教组织、联络邪教组织成员,破坏国家法律、行政法规实施。

为了维护社会主义市场经济秩序和社会管理秩序,对有下列行为之一,构成犯罪的,依照刑法有关规定追究刑事责任:

（1）利用互联网销售伪劣产品或者对商品、服务作虚假宣传。

（2）利用互联网损坏他人商业信誉和商品声誉。

（3）利用互联网侵犯他人知识产权。

（4）利用互联网编造并传播影响证券、期货交易或者其他扰乱金融秩序的虚假信息。

（5）在互联网上建立淫秽网站、网页，提供淫秽站点链接服务；或者传播淫秽书刊、影片、音像、图片。

为了保护个人、法人和其他组织的人身、财产等合法权利，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

（1）利用互联网侮辱他人或者捏造事实诽谤他人。

（2）非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密。

（3）利用互联网进行盗窃、诈骗、敲诈勒索。

利用互联网实施《全国人大常委会关于维护互联网安全的决定》第一条、第二条、第三条、第四条所列行为以外的其他行为，构成犯罪的，依照刑法有关规定追究刑事责任。

利用互联网实施违法行为，违反社会治安管理，尚不构成犯罪的，由公安机关依照《治安管理处罚法》予以处罚；违反其他法律、行政法规，尚不构成犯罪的，由有关行政管理部门依法给予行政处罚；对直接负责的主管人员和其他直接责任人员，依法给予行政处分或者纪律处分。

利用互联网侵犯他人合法权益，构成民事侵权的，依法承担民事责任。

各级人民政府及有关部门要采取积极措施，在促进互联网的应用和网络技术的普及过程中，重视和支持对网络安全技术的研究和开发，增强网络的安全防护能力。

有关主管部门要加强对互联网的运行安全和信息安全的宣传教育，依法实施有效的监督管理，防范和制止利用互联网进行的各种违法活动，为互联网的健康发展创造良好的社会环境。从事互联网业务的单位要依法开展活动，发现互联网上出现违法犯罪行为和有害信息时，要采取措施，停止传输有害信息，并及时向有关机关报告。任何单位和个人在利用互联网时，都要遵纪守法，抵制各种违法犯罪行为和有害信息。人民法院、人民检察院、公安机关、国家安全机关要各司其职，密切配合，依法严厉打击利用互联网实施的各种犯罪活动。要动员全社会的力量，依靠全社会的共同努力，保障互联网的运行安全与信息安全，促进社会主义精神文明和物质文明建设。

5.《全国人民代表大会常务委员会关于加强网络信息保护的决定》

《全国人民代表大会常务委员会关于加强网络信息保护的决定》，于 2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过。

为了保护网络信息安全，保障公民、法人和其他组织的合法权益，维护国家安全和社会公共利益，特作以下决定：

（1）国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。

（2）网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同

意，不得违反法律、法规的规定和双方的约定收集、使用信息。网络服务提供者和其他企业事业单位收集、使用公民个人电子信息，应当公开其收集、使用规则。

（3）网络服务提供者和其他企业、事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

（4）网络服务提供者和其他企业、事业单位应当采取技术措施和其他必要措施，确保信息安全，防止在业务活动中收集的公民个人电子信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施。

（5）网络服务提供者应当加强对其用户发布的信息的管理，发现法律、法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

（6）网络服务提供者为用户办理网站接入服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。

（7）任何组织和个人未经电子信息接收者同意或者请求，或者电子信息接收者明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。

（8）公民发现泄露个人身份、散布个人隐私等侵害其合法权益的网络信息，或者受到商业性电子信息侵扰的，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止。

（9）任何组织和个人对窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为，有权向有关主管部门举报、控告；接到举报、控告的部门应当依法及时处理。被侵权人可以依法提起诉讼。

（10）有关主管部门应当在各自职权范围内依法履行职责，采取技术措施和其他必要措施，防范、制止和查处窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为。有关主管部门依法履行职责时，网络服务提供者应当予以配合，提供技术支持。国家机关及其工作人员对在履行职责中知悉的公民个人电子信息应当予以保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

（11）对有违反本决定行为的，依法给予警告、罚款、没收违法所得、吊销许可证或者取消备案、关闭网站、禁止有关责任人员从事网络服务业务等处罚，记入社会信用档案并予以公布；构成违反治安管理行为的，依法给予治安管理处罚。构成犯罪的，依法追究刑事责任。侵害他人民事权益的，依法承担民事责任。

（12）本决定自公布之日起施行。

10.2 信息安全国家政策

10.2.1 国家信息安全保障总体方针

国家信息安全保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安

全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。信息系统的安全保护等级分为5级。

国家有关政策规定的加强信息安全保障工作，主要遵循下述原则：

（1）基于安全需求原则。

组织机构应根据其信息系统担负的使命，积累的信息资产的重要性，可能受到的威胁及面临的风险分析安全需求，按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，从全局上恰当地平衡安全投入与效果。

（2）主要领导负责原则。

主要领导应确立其组织统一的信息安全保障的宗旨和政策，负责提高员工的安全意识，组织有效安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效。

（3）全员参与原则。

信息系统所有相关人员应普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全。

（4）系统方法原则。

按照系统工程的要求，识别和理解信息安全保障相互关联的层面和过程，采用管理和技术结合的方法，提高实现安全保障的目标的有效性和效率。

（5）持续改进原则。

安全管理是一种动态反馈过程，贯穿整个安全管理的生存周期，随着安全需求和系统脆弱性的时空分布变化、威胁程度的提高、系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性。

（6）依法管理原则。

信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响。

（7）分权和授权原则。

对特定职能或责任领域的管理功能实施分离、独立审计等实行分权，避免权力过分集中所带来的隐患，以减小未授权的修改或滥用系统资源的机会。任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必需的权限，不应享有任何多余权限。

（8）选用成熟技术原则。

成熟的技术具有较好的可靠性和稳定性，采用新技术时要重视其成熟的程度，并应首先局部试点，然后逐步推广，以减少或避免可能出现的失误。

（9）分级保护原则。

按等级划分标准确定信息系统的安全保护等级，实行分级保护；对多个子系统构成的大型信息系统，确定系统的基本安全保护等级，并根据实际安全需求，分别确定各子系统的安全保护等级，实行多级安全保护。

（10）管理与技术并重原则。

坚持积极防御和综合防范，全面提高信息系统安全防护能力，立足国情，采用管理与技

术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标。

(11) 自我保护和国家监管结合原则。

对信息系统安全实行自我保护和国家监管相结合。组织机构要对自己的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护能力和水平，保障国家信息安全。

10.2.2 电子政府与重要信息系统信息安全政策

电子政府是指通过整合运用包括互联网等 IT 技术，实现迅速、透明、方便和高效地处理行政机关之间(G2G)、行政机关与公民之间(G2C)及行政机关与企业之间(G2B)的全部业务的电子化的政府。

电子政府的目的是政府利用 IT 技术实现向全社会提供信息和服务的电子化，使全社会得到更充分、快捷、高效的信息和服务。

从目前我国电子政务立法的总体情况看，电子政务的立法还处于一个摸索状态，具体表现为纲领性立法尚未出台、各部门立法尚待加速完善。

首先，我国电子政务的立法状况正处于一个"无纲领性立法，无明确的立法规划，无有效的立法评价及监督机制"的三无状态。至今我国尚未出台关于电子政务的纲领性法律，且更为严重的是尚无明确的立法规划，就更不用说评价及监督立法的机制了。

其次，我国多数电子政务立法的效力层次低，效力层次较高的法律、行政法规尚未出台。例如，《电子商务监督管理暂行办法》只是一部由北京市工商行政管理局颁布施行的地方政府部门规章；已首次提交广东省九届人大常委会审议的《广东省电子交易条例(草案)》也仅是一部地方规章。

加强政府信息系统安全和保密管理工作，应坚持四项基本要求：明确职责、强化人员培训、完善安全措施和手段、加强信息安全检查。

10.2.3 风险评估有关政策规范

识别了机构的信息资产及其威胁和漏洞后，就可以评估每个漏洞的相关风险了。这是通过风险评估过程来完成的。风险评估给每项信息资产分配一个风险等级或者分数。此数字在绝对术语中没有任何意义，但可用于评估每项易受攻击的信息资产的相关风险，并在风险控制过程中促进比较等级的发展。

有关信息安全风险评估工作，都应遵循以下国家颁布的文件要求，该类文件包括：《计算机信息安全要求》(GB/T 9361)；《计算机信息系统安全保护等级划分准则》(GB 17859—1999)；《信息技术、安全技术、信息技术安全性评估准则》(GB/T 18336—2001)(IDT ISO/IEC 15408：1999)；《信息技术信息安全管理实用规则》(GB/T 19716—2005)(ISO/IEC 17799—2000，MOD)。

10.2.4 等级保护有关政策规范

等级保护主要依据《信息安全等级保护管理办法》的有关要求进行，其中的主要内容

包括：

第六条　国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

第七条　信息系统的安全保护等级分为五级：

第一级，信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级，信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级，信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级，信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第五级，信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

第八条　信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

10.3　信息安全从业人员道德规范

计算机职业道德是指在计算机行业及其应用领域所形成的社会意识形态和伦理关系下，调整人与人之间、人与知识产权之间、人与计算机之间以及人和社会之间关系的行为规范总和。

增强职业道德规范是计算机信息安全中人员安全的一个重要内容，是法律行为规范的补充，是非强制性的自律要求，其目的是用来规范各类信息的使用。

信息安全从业人员基本道德规范：

(1) 保障因特网的运行安全方面。

(2) 维护国家安全和社会稳定方面。

(3) 维护社会主义市场经济秩序和社会管理秩序方面。

(4) 保护个人、法人和其他组织的人身、财产等合法权利方面。

注册信息安全专业人员必须严格履行其职责并遵守以下道德准则：

(1) 所有注册信息安全专业人员(CISP)都必须付出努力才能注册。为贯彻这条原则，所有的 CISP 都必须承诺完全遵守道德准则。

(2) CISP 必须诚实、公正、负责、守法。

(3) CISP 必须勤奋和胜任工作，不断提高自身专业能力和水平。

(4) CISP 必须保护信息系统、应用程序和系统的价值。

(5) CISP 必须接受中国信息安全测评中心(CNITSEC)的监督。在任何情况下，不损

害 CNITSEC 的声誉,对 CNITSEC 针对 CISP 而进行的调查应给予充分的合作。

(6) CISP 必须按规定向 CNITSEC 交纳费用。

10.4 通行道德规范

不管是一名计算机工作人员还是一名普通群众,都应该培养正确的道德观念,严格遵守计算机与因特网的使用道德规范,因为因特网最大的特点就开放性和自主性。在因特网上,非常自由,你想说什么就可以说什么,你想做什么就可以做什么。当然,这得有一定的限度,不仅不能侵犯国家的利益和大多数人的利益,也得与广大网民们友好相处,受到大家的尊重。因此,除了制定各种法规外,培养良好的道德规范也是非常重要的。

计算机使用应遵守以下道德规范:

(1) 不破坏别人的计算机系统资源。

(2) 不制造传播病毒程序。

(3) 不窃取别人的软件资源。

(4) 不破译别人的口令或密码。

(5) 不使用带病毒的软件,更不向别人提供带病毒的软件。

(6) 坚持使用正版软件。

因特网使用应遵守中国互联网协会《文明上网自律公约》,其主要内容如下:

自觉遵纪守法,倡导社会公德,促进绿色网络建设;

提倡先进文化,摒弃消极颓废,促进网络文明健康;

提倡自主创新,摒弃盗版剽窃,促进网络应用繁荣;

提倡互相尊重,摒弃造谣诽谤,促进网络和谐共处;

提倡诚实守信,摒弃弄虚作假,促进网络安全可信;

提倡社会关爱,摒弃低俗沉迷,促进少年健康成长;

提倡公平竞争,摒弃尔虞我诈,促进网络百花齐放;

提倡人人受益,消除数字鸿沟,促进信息资源共享。

10.5 本章小结

通过本章的学习,读者应该增强自觉遵守与信息活动相关的法律法规的意识,负责任地参与信息实践。在使用因特网的过程中,认识网络使用规范和有关伦理道德的基本内涵;能够识别并抵制不良信息;树立网络交流中的安全意识;了解信息技术可能带来的不利于身心健康的因素,养成健康使用信息技术的习惯。在空余时间应该多学习相关法律法规知识,充实自己。

参 考 文 献

[1] 王春东.信息安全管理 [M].武汉：武汉大学出版社，2008.
[2] 黄波，刘洋洋.信息网络安全管理 [M].北京：清华大学出版社，2013.
[3] 张基温.信息系统安全教程[M].北京：清华大学出版社，2007.
[4] 王群.计算机网络安全管理[M].北京：人民邮电出版社，2010.
[5] 谢宗晓，刘琦.信息安全管理体系实施案例及文件集[M].北京：中国标准出版社，2010.
[6] 中国信息安全认证中心. 信息安全管理体系审核指南 [M].北京：中国标准出版社，2012.
[7] 张泽虹，赵冬梅.信息安全管理与风险评估[M].北京：电子工业出版社，2010.
[8] 吕俊杰. 信息安全风险管理方法及应用[M].北京：知识产权出版社，2010.
[9] 付永钢. 计算机信息安全技术[M].北京：清华大学出版社，2012.
[10] 唐成华.信息安全工程与管理[M].西安：西安电子科技大学出版社，2012.
[11] 李继国，余纯武.信息安全数学基础[M].武汉：武汉大学出版社，2006.
[12] 胡爱群，蒋睿，陆哲明.网络信息安全理论与技术[M].武汉：华中科技大学出版社，2008.
[13] 王宇，阎慧.信息安全保密技术[M].北京：国防工业出版社，2010.
[14] 范红，胡志昂，金丽娜.信息系统等级保护安全设计技术实现与使用[M].北京：清华大学出版社，2010.
[15] 蒋文保.信任管理与网络安全[M].北京：清华大学出版社，2012.
[16] 中国信息安全测评中心.信息安全积极防御技术[M].北京：航空工业出版社，2009.
[17] 胡志昂，范红.信息系统等级保护安全建设技术方案设计实现与应用[M].北京：电子工业出版社，2009.
[18] 林幼槐，信息通信网络建设安全管理概要[M].北京：人民邮电出版社，2012.
[19] 谢宗晓.信息安全管理体系实施案例[M].北京：中国标准出版社，2012.
[20] 吴世忠.信息安全技术[M].北京：机械工业出版社，2014.
[21] 田俊峰.可信计算与信任管理[M].北京：科学出版社，2014.
[22] 张浩军，杨卫东，谭玉波.信息安全技术基础[M].北京：中国水利水电出版社，2011.
[23] 潘明惠.网络信息安全工程原理与应用[M].北京：清华大学出版社，2011.
[24] 迟俊鸿，崔炜.网络信息安全项目教程[M].北京：电子工业出版社，2010.
[25] 中国石化.信息安全技术与应用[M].北京：中国石化出版社，2012.